

1. Barracuda SSL VPN - Overview	3
1.1 Barracuda SSL VPN Release Notes 2.4	3
1.2 Deployment	5
1.2.1 Hardware Specifications	7
1.2.2 Virtual Systems	8
1.2.2.1 Sizing CPU, RAM, and Disk for Your Barracuda SSL VPN Vx	9
1.2.2.2 How to Deploy Barracuda SSL VPN Vx Virtual Images	10
1.2.2.3 How to Enable Promiscuous Mode on VMware for the Barracuda Network Connector	11
1.2.2.4 Barracuda SSL VPN Vx Quick Start Guide	13
1.2.3 High Availability Deployment	16
1.2.3.1 How to Configure a High Availability Cluster	16
1.2.4 Licensing	18
1.3 Getting Started	18
1.4 Administrative Interfaces	20
1.5 Access Control	21
1.5.1 How to Create and Modify User Databases	22
1.5.1.1 Example - Create a User Database with Active Directory	23
1.5.2 Authentication Schemes	24
1.5.2.1 Hardware Token Authentication	25
1.5.2.2 How to Configure One-Time Password (OTP) Authentication	26
1.5.2.3 How to Configure Public Key Authentication	27
1.5.2.4 How to Configure SSL Client Certificate Authentication	28
1.5.2.5 Example - How to Install and Configure YubiRADIUS	29
1.5.2.6 Example - Authentication with SMS Passcode RADIUS server	40
1.5.3 How to Configure Policies	42
1.5.4 Access Rights	43
1.6 Resources	44
1.6.1 Web Forwards	44
1.6.1.1 Custom Web Forwards	44
1.6.1.1.1 How to Create Custom Web Forwards	47
1.6.1.2 How to Configure a Microsoft SharePoint Web Forward	48
1.6.1.3 How to Configure a Microsoft Exchange OWA Web Forward	49
1.6.2 Network Places	49
1.6.2.1 How to Create a Network Place Resource	50
1.6.2.2 How to Configure AV Scanning	51
1.6.3 Applications	51
1.6.3.1 How to Create an Application Resource	52
1.6.3.2 How to Configure Outlook Anywhere	53
1.6.3.3 How to Configure ActiveSync for Microsoft Exchange Servers	55
1.6.3.4 How to Configure Microsoft RDP RemoteApp	56
1.6.4 SSL Tunnels	57
1.6.4.1 How to Create an SSL Tunnel	58
1.6.5 Remote Assistance	59
1.6.5.1 Requesting Remote Assistance	59
1.6.5.2 Providing Remote Assistance	60
1.6.6 Network Connector	61
1.6.6.1 How to Configure the Network Connector	61
1.6.6.2 How to Create a Static Route	62
1.6.6.3 Advanced Network Connector Client Configuration	63
1.6.6.4 Using the Network Connector with Microsoft Windows	65
1.6.6.5 Using the Network Connector with Mac OS X	66
1.6.6.6 Using the Network Connector with Linux	67
1.6.7 How to Configure IPsec	68
1.6.7.1 How to Configure Mobile Devices	69
1.6.7.2 How to Configure Remote Devices	71
1.6.8 How to Configure PPTP	73
1.6.9 How to Configure Profiles	74
1.6.10 Provisioning Client Devices	74
1.7 Advanced Configuration	77
1.7.1 Attributes	77
1.7.2 Messaging	77

1.7.3 Agents	78
1.7.3.1 How to Configure a Server Agent	78
1.7.3.2 How to Configure the SSL VPN Agent	80
1.8 Monitoring	80
1.8.1 Basic Monitoring	80
1.8.2 Notifications	82
1.8.3 SNMP	83
1.9 Maintenance	84
1.9.1 How to Configure Automated Backups	84
1.9.2 Restore from Backups	84
1.9.3 Update Firmware	85
1.9.4 How to Update the Firmware in a High Availability Cluster	86
1.10 Limited Warranty and License	87

Barracuda SSL VPN - Overview

The Barracuda SSL VPN is an ideal appliance for giving remote users secure access to network resources. The Barracuda SSL VPN only requires a browser to give remote users access from any computer. Built-in and third-party multi-factor authentication and network access control (NAC) only connects clients that meet chosen security standards. For secure remote access through smartphones and other mobile devices, the Barracuda SSL VPN supports both L2TP/IPsec and PPTP. The Barracuda SSL VPN is available as a hardware and a virtual appliance.

Where to Start

If you have the Barracuda SSL VPN Vx virtual appliance, start here:

- [Barracuda SSL VPN Vx Quick Start Guide](#)
- [Getting Started](#)

If you have the Barracuda SSL VPN appliance, start here:

- [Quick Start Guide for version 2.4 \(PDF\)](#) or [Quick Start Guide for version 2.3 \(PDF\)](#)
- [Getting Started](#)

Key Features

- [Access Control](#) – A multi-factor authentication process, with support for external authentication and third-party hardware tokens, combined with NAC and multiple user databases.
- [Web Forwards](#) – Make intranet resources available for your remote users and secure unencrypted connections before they leave the network.
- [Network Places](#) – Provide remote users with a secure web interface to access corporate network file shares.
- [Applications](#) – Provide applications to remote client systems through the Barracuda SSL VPN Agent for remote access.
- [SSL Tunnels](#) – Create SSL Tunnels to allow secure connections from remote devices to the Barracuda SSL VPN by encrypting data for client/server applications.
- [Network Connector](#) – An application that provides full, transparent network access for users requiring widespread network access.
- [L2TP/IPsec / PPTP](#) – Configure secure remote access through smartphones and other mobile devices.

Barracuda SSL VPN Release Notes 2.4



Please Read Before Updating

Before installing any firmware version, be sure to make a backup of your configuration and read all release notes that apply to versions more recent than the one currently running on your system.

Do not manually reboot your system at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support. The update process typically takes only a few minutes after the update is applied. The appliance web interface for the administrator will usually be available a minute or two before the SSL VPN user interface. If the process takes longer, please contact Technical Support for further assistance.

Upgrading to Version 2.x

- **When upgrading from version 2.3 (or earlier) firmware:**
 - Backups taken from earlier firmware versions will NOT restore properly with the new backup/restore functionality found starting in version 2.4. Make new backups after the firmware update.
- **Mapped Drives:**
 - WebDAV is now the default method for providing Mapped Drives and configuration settings have been changed accordingly. Windows 7 and Vista 64-bit clients will be prompted to uninstall the current Dokan driver and also given the option to increase the maximum file download size to 2GB when launching Mapped Drives.
 - Client Certificates will need to be disabled when launching WebDAV Mapped Drives.
 - Version 2.3.1.013 is not compatible with systems that are clustered.
- **When upgrading from version 2.1 firmware:**
 - Replacement Proxy Web Forwards for OWA that were created prior to version 2.2 are no longer supported. If you have one, you will need to replace it using the new OWA Template. Go to the RESOURCES > Web Forwards page and delete the old Web Forward. Then create a new one using the Mail Web Forward category.

- When configuring Barracuda Network Connector on Macintosh systems, note that DNS insertion and Up/Down commands are mutually exclusive.

What's new with the Barracuda SSL VPN Version 2.4.0.12

- Fix: Clustering on new systems [BNVS-4678]
- Fix: High severity vulnerability: non-persistent XSS [BNSEC-2802 / BNVS-4542]
- Fix: High severity vulnerability: persistent XSS [BNSEC-2697 / BNVS-4543]
- Fix: Unknown severity vulnerability: [BNSEC-380]
- Fix: Unknown severity vulnerability: [BNSEC-335]

What's new with the Barracuda SSL VPN Version 2.4.0.10

- Fix: External access blocked for non SSH ports [BNVS-4152]
- Fix: The most recent Scheduled Backup files are retained [BNVS-4614]
- Fix: High severity vulnerability: Unauthenticated, non-persistent XSS [BNSEC-1546 / BNVS-4210]
- Fix: High severity vulnerability: Unauthenticated, non-persistent XSS [BNSEC-1542 / BNVS-4211]
- Fix: High severity vulnerability: Clickjacking [BNSEC-509 / BNVS-4024]
- Fix: Med severity vulnerability: Cross Site Request Forgery (CSRF) [BNSEC-1247 / BNVS-4079]
- Fix: Med severity vulnerability: URL Redirection [BNSEC-727 / BNVS-3665]
- Fix: Low severity vulnerability: Requires a man in the middle, url redirection [BNSEC-1399 / BNVS-4147]
- Fix: Low severity vulnerability: Requires authentication, non-persistent XSS [BNSEC-1239 / BNVS-4078]
- Fix: Low severity vulnerability: Cross Site Request Forgery (CSRF), HTTP header injection, non-persistent X SS [BNSEC-1144 / BNVS-4026]

What's new with the Barracuda SSL VPN Version 2.4.0.9

New Features

- The Device Configuration feature allows resources and other settings configured on the Barracuda SSL VPN to be provisioned directly to a user's device.
- Improved Sharepoint functionality, including supporting Sharepoint 2013.
- Policy time restrictions are more comprehensive.
- Improved browser NAC checking.
- Download functionality for all aspects of the system works faster and more reliably.
- Increased backup and restore capabilities (from the appliance interface).

Version 2.4.0.9 Fixes:

- **Backups**
 - Show All Backups option on the ADVANCED > Backups page displays all backup files on the share [BNVS-4348]
 - Only the requested number of SMB backups is stored [BNVS-4378]
 - Status of SMB backup is reported accurately [BNVS-4376]
 - Clustering information is excluded from backups [BNVS-4382]
- **Other**
 - All Network Connector client configurations can be launched from the user interface [BNVS-4381]
 - Fixed Java applet signing to conform to new security in Java 1.7u45 [BNVS-4516]

Note: This error may still appear if the SSLVPN doesn't have a valid SSL certificate installed. A valid SSL certificate will be required for all SSL VPN devices as of the release of Java 1.7u51

Version 2.4.0.7:

- Fix: Mapped drives time out according to the inactivity timeout setting under Profiles [BNVS-4337]
- Fix: Attempts to access hosts not in the Web Forward Allowed Hosts list displays error message [BNVS-4319]
- Fix: Can log off users with Network Connector sessions using the Sessions page [BNVS-4322]
- Fix: Set limitations on IP subnet range for PPTP and IPSec [BNVS-4325]
- Fix: Updated Code Signing Certificate
- Fix: Vulnerability - Information Disclosure [BNSEC-1839 / BNVS-4261]
- Fix: Vulnerability - Unauthenticated, XSS-Not Persistent [BNSEC-1542 / BNVS-4211]
- Fix: Vulnerability - Unauthenticated, XSS-Not Persistent [BNSEC-1546 / BNVS-4210]
- Fix: Vulnerability - Requires Man in the Middle, URL Redirection [BNSEC-1399 / BNVS-4147]
- Fix: Vulnerability - CSRF [BNSEC-1247 / BNVS-4079]

- Fix: Vulnerability - Authenticated, XSS-Not Persistent [BNSEC-1239 / BNVS-4078]
- Fix: Vulnerability - CSRF, HTTP Header Injection, XSS-Not Persistent [BNSEC-1144 / BNVS-4026]
- Fix: Vulnerability - Click Jacking [BNSEC-509 / BNVS-4024]
- Fix: Vulnerability - URL Redirection [BNSEC-727 / BNVS-3665]

Version 2.4.0.3:

- Feature: Bookmark aliases are created automatically for new and existing resources
- Fix: Server Agent service starts on Linux [BNVS-4244]
- Fix: Improved ActiveSync session disconnection handling [BNVS-4243, BNVS-4263]
- Fix: Prevent files that were in tmp directory from being deleted when they should not have been [BNVS-4188]
- Fix: Enabled uploading of certificates with PKCS #8 private keys [BNVS-4235]
- Fix: Account selection works correctly for Read Only mode Active Directory groups when using Internet Explorer [BNVS-4217]
- Fix: My Resources filter displays correct selection [BNVS-4258]
- Fix: Creating a new Certificate Authority is possible after deleting an existing one [BNVS-4233, BNVS-4255]
- Fix: Ssladmin session information is displayed correctly on clustered systems [BNVS-4225]
- Fix: Correction to AD password expiry message [BNVS-3591]
- Fix: Improvements to Microsoft Sharepoint 2013 checkout discard in Microsoft Office 2007 and 2010 [BNVS-4184]

Version 2.4.0.2 Fixes:

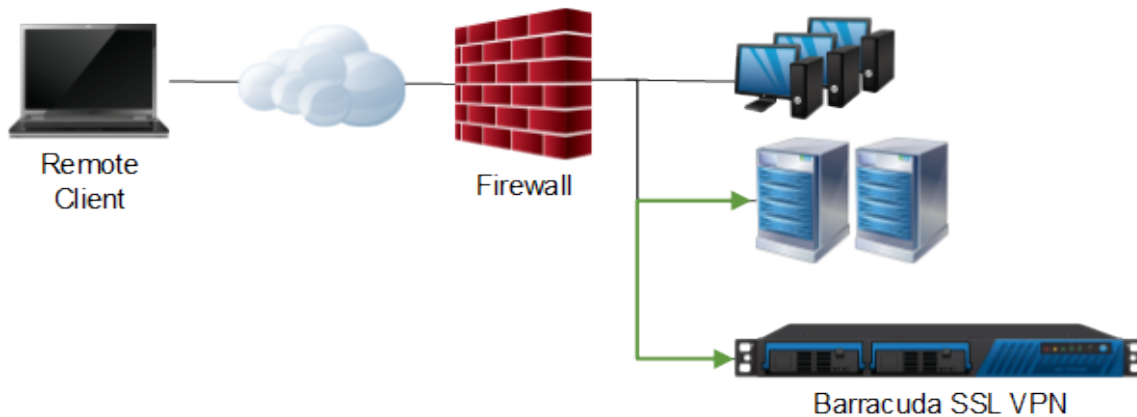
- **Graphs**
 - Graphs display correctly in Internet Explorer version 10 [BNVS-4030]
- **Web Forwards**
 - Path based web forwards display large pages containing multi-byte characters accurately [BNVS-4196]
 - Web sites that switch between character encodings display extended chars (?, ?, etc.) correctly [BNVS-4102]
 - Launching a Host File Redirect Tunneled Web Forward in Windows 7 closes the Command prompt window [BNVS-4101]
 - Sharepoint 2010 documents can be edited [BNVS-4132]
- **IPsec/PPTP**
 - Timeout option added for IPsec/PPTP sessions [BNVS-4155]
 - When launching PPTP, if the connection already exists then a confirmation message is not displayed [BNVS-4194]
 - IPsec PSK can include all valid symbols [BNVS-4081, BNVS-4125]
- **Mapped Drives**
 - Webdav Mapped Drives do not timeout due to inactivity [BNVS-4090]
 - Session timeout will disconnect Mapped Drives [BNVS-4128]
 - Office 2013 documents work with Mapped Drives [BNVS-3778]
- **Sessions**
 - Password can be entered after session has been locked due to browser closure [BNVS-4144]
- **Server Agent**
 - The ADVANCED > Server Agents page refreshes correctly when an agent is enabled or disabled in Internet Explorer version 10 [BNVS-4119]
 - Zip file containing the server agent client contains the correct version [BNVS-4120]
 - Server Agent service starts on Linux [BNVS-4244]
- **Other**
 - Improved notifications message handling under heavy load [BNVS-4058]
 - NAC antivirus checking detects status of multiple installed AV products [BNVS-4099]
 - Network Connector routes can be added in Mac OS X [BNVS-4100]
 - Authentication schemes and NAC exceptions consider policy time restrictions [BNVS-3455]
 - /32 CIDR notation is handled correctly by IP authentication [BNVS-3818]

Deployment

The Barracuda SSL VPN is typically deployed in the following configurations:

- **Direct Access DMZ Deployment** – Behind the firewall, with direct access to all intranet resources.
- **Multilayer Firewall DMZ Deployment** – In a DMZ between the external and internal firewall. Additional ports have to be opened on the internal firewall to access internal resources.
- **Isolated Deployment** – The Barracuda SSL VPN is reachable from the Internet. All resources connect via Server Agents which initiate the connection from inside the networks. No ports have to be opened.

Direct Access DMZ Deployment



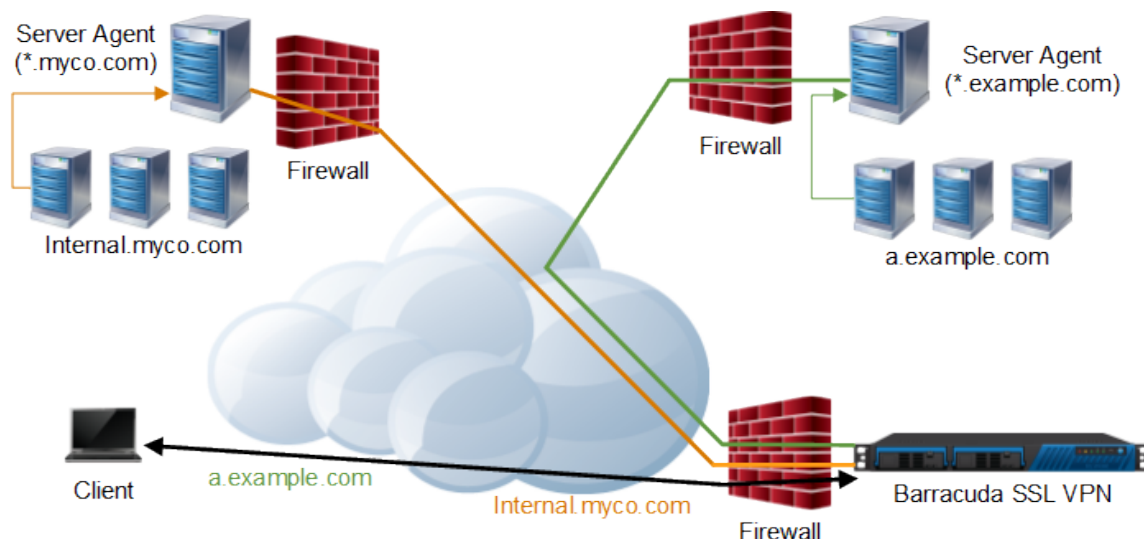
The Barracuda SSL VPN is deployed behind the firewall. Only one port (443) has to be opened up by the firewall and forwarded to the SSL VPN. You have direct access to all services (authentication, file, web, etc.) in the intranet without further configuration.

Multilayer Firewall DMZ Deployment



The Barracuda SSL VPN is deployed in a DMZ behind the corporate firewall but before the internal network firewall. All access to services on the internal network requires ports to be opened on the internal firewall. By deploying the Barracuda SSL VPN between the two firewalls, another security layer is added. It is also possible to install the Server Agent on a computer in the internal network, which initiates an SSL tunnel on port 443 from the inside of the network so you can limit the ports that you must open on the internal firewall.

Isolated Deployment



The Barracuda SSL VPN is deployed and isolated from the rest of the network. All resources are located in networks which are not directly accessible by the Barracuda SSL VPN. Server Agents inside the networks initiate tunnels to the SSL VPN and act as proxies for the local resources. This deployment minimizes security implications caused by opening various ports on the firewalls to access the resources located behind them.

In this Section

- [Hardware Specifications](#)
- [Virtual Systems](#)
- [High Availability Deployment](#)
- [Licensing](#)

Hardware Specifications



Warranty and Safety Instructions

Unless you are instructed to do so by Barracuda Networks Technical Support, you will void your warranty and hardware support if you open your Barracuda Networks appliance or remove its warranty label.

[Barracuda Networks Appliance Safety Instructions Hardware Compliance.](#)



Hardware Specifications of the Various Barracuda SSL VPN Models



The hardware configuration list in this table was valid at the time this content was created. The listed components are subject to change at any time, as Barracuda Networks may change hardware components due to technological progress. Therefore, the list may not reflect the current hardware configuration of the Barracuda SSL VPN.

	Barracuda SSL VPN Model					
	180	280	380	480	680	880
Recommended Maximum Concurrent Users	15	25	50	100	500	1,000
Hardware						
Rackmount Chassis	1U Mini	1U Mini	1U Mini	1U Mini	1U Full-size	1U Full-size
Dimensions (inches)	16.8 x 1.7 x 9	16.8 x 1.7 x 9	16.8 x 1.7 x 14	16.8 x 1.7 x 14	16.8 x 1.7 x 22.6	17.4 x 3.5 x 25.5
Weight (lbs)	8	8	12	12	26	46
Ethernet	1 x 10 / 100	1x Gigabit	1x Gigabit	1x Gigabit	2x Gigabit	2x Gigabit
AC Input Current (Amps)	1.0	1.0	1.2	1.4	1.8	4.1
Redundant Disk Array (RAID)	No	No	No	Yes	Yes	Yes
ECC Memory	No	No	No	No	Yes	Yes
Redundant Power Supply	No	No	No	No	No	Hot Swap

Features						
SSL Tunneling	Yes	Yes	Yes	Yes	Yes	Yes
Barracuda Network Connector	Yes	Yes	Yes	Yes	Yes	Yes
Intranet Web Forwarding	Yes	Yes	Yes	Yes	Yes	Yes
Windows Explorer Mapped Drives	Yes	Yes	Yes	Yes	Yes	Yes
Citrix XenApp/VNC/NX /Telnet/ SSH/RDP Applications	Yes	Yes	Yes	Yes	Yes	Yes
Remote Desktop Single Sign-On	Yes	Yes	Yes	Yes	Yes	Yes
Antivirus	Yes	Yes	Yes	Yes	Yes	Yes
L2TP/IPsec, PPTP Mobile Device Support	Yes	Yes	Yes	Yes	Yes	Yes
Client Access Controls	Yes	Yes	Yes	Yes	Yes	Yes
Active Directory/LDAP Integration	Yes	Yes	Yes	Yes	Yes	Yes
Layered Authentication Schemes	Yes	Yes	Yes	Yes	Yes	Yes
Remote Assistance	No	No	Yes	Yes	Yes	Yes
Multiple User Realms	No	No	Yes	Yes	Yes	Yes
Barracuda SSL VPN Server Agent	No	No	Yes	Yes	Yes	Yes
Hardware Token Support	No	No	Yes	Yes	Yes	Yes
RADIUS Authentication	No	No	Yes	Yes	Yes	Yes
Syslog Logging	No	No	Yes	Yes	Yes	Yes
SNMP/API	No	No	No	Yes	Yes	Yes
Clustering/High Availability	No	No	No	Yes	Yes	Yes

Virtual Systems

The Barracuda SSL VPN is available as a virtual appliance. Because it is mostly used after office hours, it is suitable on a server hosting virtual machines that are used intensely during office hours but sit idle for the rest of the time. You can pair a Barracuda SSL VPN Vx with a hardware Barracuda SSL VPN appliance to create a high availability cluster. With a load balancer, you can create a configuration that uses the resources of the hardware Barracuda SSL VPN during the day when the hypervisor is under high load and then use the virtual Barracuda SSL VPN to cover the peak load in the evening when employees log in from home.

Deploying the Barracuda SSL VPN Vx

To deploy the Barracuda SSL VPN Vx, complete the following tasks:

1. [Size the CPU, RAM, and Disk for your Barracuda SSL VPN Vx.](#)
2. [Deploy the Barracuda SSL VPN Vx virtual images.](#)
3. (For VMware hypervisors) [Enable Promiscuous mode on VMware for the Barracuda Network Connector.](#)
4. [Set up the Barracuda SSL VPN Vx with the Quick Start Guide.](#)

Sizing CPU, RAM, and Disk for Your Barracuda SSL VPN Vx

Barracuda Networks recommends the following sizing for the initial deployment of your virtual appliance or the upgrade of existing installations.

Virtual Machine Sizing Requirements

Barracuda SSL VPN Vx Model	Licensed Cores	Recommended RAM	Recommended Hard Disk Space
V180	1	1 GB	50 GB
V380	2	1 GB	50 GB
V480	3	2 GB	50-200 GB
V680	4	4 GB	200-500 GB
V680 + additional cores license	Limited only by license	1 GB per core	500+ GB

Provisioning CPUs/Cores

You must provision the number of cores in your hypervisor before the Barracuda SSL VPN Vx can use them. Each model can only use a set number of cores. For example, if you assign 6 cores to the Barracuda SSL VPN Vx 380 (which can only use 2 cores), the virtual machine turns off the extra cores that cannot be used.

To add cores:

1. Shut down your hypervisor.
2. Go into the virtual machine settings.
3. Add CPUs. The number of available CPUs that are shown will vary with your hypervisor licensing and version. In some cases, the number of CPUs that you can add must be a multiple of 2.

Provisioning Hard Drives

Provision your hard disk space according to the [Virtual Machine Sizing Requirements](#) table. Barracuda Networks requires a minimum of 50 GB of hard disk space to run your Barracuda SSL VPN Vx.

From your hypervisor, you can either edit the provisioned size of the hard drives or add a hard drive.



Recommended VMware Provisioning Format

If you are using VMware, note that VMware tools support thin provisioning, which is not currently available in the virtual product lines. Barracuda Networks recommends using the **THICK** provisioning format when allocating disk storage for your Barracuda Networks virtual machine.

To add a hard drive:

1. Shut down your Barracuda SSL VPN Vx.

2. Take a snapshot of your virtual machine.
3. Edit the settings in your virtual machine, and either increase the size of the hard drive or add a new hard drive.
4. Restart the virtual machine.
5. During the system bootup, answer **Yes** after the pop-out console displays a message asking if you want to use the new additional space. If you do not respond in 30 seconds, the pop-out console times out and defaults to **No**. Resizing can take several minutes, depending on the amount of provisioned hard drive space.

How to Deploy Barracuda SSL VPN Vx Virtual Images

Barracuda offers three types of packages for virtual deployment. Follow the instructions for your hypervisor to deploy the Barracuda SSL VPN Vx appliance.

Package Type	Hypervisors
OVF images	• VMware ESX and ESXi 3.5 • VMware ESX and ESXi 4.x • Sun/Oracle VirtualBox and VirtualBox OSE 3.2
VMX images	• VMware Server 2.0+ • VMware Player 3.0+ • VMware Workstation 6.0 + • VMware Fusion 3.0+
XVA images	• Citrix Xen Server 5.5+



If you are deploying the Barracuda SSL VPN Vx on a VMware hypervisor, complete [How to Enable Promiscuous Mode on VMware for the Barracuda Network Connector](#) after deploying the VM.

Deploying OVF Images

VMware ESX and ESXi 3.5

Use the OVF file ending in **-35.ovf** for this hypervisor.

1. From the **File** menu in the VMware Infrastructure client, select **Virtual Appliance > Import**.
2. Select **Import from file**, and navigate to the **BarracudaSSLVPN-vm<version#>-fw__FIRMWARE__-<version#>.ovf** file.
3. Click **Next** to review the appliance information, review the End User License Agreement, and give the virtual appliance a name that is useful to your environment.
4. Click **Finish**.
5. After your appliance finishes importing, right-click it, select **Open Console**, and then click the green arrow to power on the virtual appliance.
6. Follow the [Quick Start Guide](#) instructions to provision your Barracuda SSL VPN Vx appliance.

VMware ESX and ESXi 4.x

Use the OVF file ending in **-4x.ovf** for this hypervisor.

1. From the **File** menu in the vSphere client, select **Deploy OVF Template**.
2. Select **Import from file**, and navigate to the **BarracudaSSLVPN-vm3.1.0-fw__FIRMWARE__-20120327-4x.ovf** file.
3. Click **Next** to review the appliance information, review the End User License Agreement, and give the virtual appliance a name that is useful to your environment. Set the network to point to the target network for this virtual appliance.
4. After your appliance finishes importing, right-click it, select **Open Console**, and then click the green arrow to power on the virtual appliance.
5. Follow the [Quick Start Guide](#) instructions to provision your Barracuda SSL VPN Vx appliance.

Sun/Oracle VirtualBox and VirtualBox OSE 3.2

Use the OVF file ending in **-4x.ovf** for this hypervisor.

1. From the **File** menu in the VirtualBox client, select **Import Appliance**.
2. Navigate to the **BarracudaSSLVPN-vm3.1.0-fw__FIRMWARE__-20120327-4x.ovf** file.
3. Use the default settings for the import, and click **Finish**.
4. Start the appliance.

5. Follow the [Quick Start Guide](#) instructions to provision your Barracuda SSL VPN Vx appliance.

Deploying VMX Images

VMware Server 2.x

1. Put the files ending in. **vmx** and. **vmdk** into a folder in your datastore (which you can locate from the **Datastores** list on your server's summary page).
2. From the VMware Infrastructure Web Access client's **Virtual Machine** menu, select **Add Virtual Machine to Inventory**.
3. Navigate to the folder used in step 1, and click the **BarracudaSSLVPN.vmx** file from the list under **Contents**.
4. Click **OK**.
5. Start the appliance.
6. Follow the [Quick Start Guide](#) instructions to provision your Barracuda SSL VPN Vx appliance.

VMware Player 3.x



VMware Player cannot edit the network / vswitch settings. This can cause problems when testing the Network Connector.

1. From the **File** menu, select **Open a Virtual Machine**.
2. Navigate to the **BarracudaSSLVPN.vmx** file.
3. Use the default settings, and click **Finish**.
4. Start the appliance.
5. Follow the [Quick Start Guide](#) instructions to provision your Barracuda SSL VPN Vx appliance.

VMware Workstation 6.x

1. From the **File** menu, select **Open a Virtual Machine**.
2. Navigate to the **BarracudaSSLVPN.vmx** file.
3. Use the default settings, and click **Finish**.
4. Start the appliance.
5. Follow the [Quick Start Guide](#) instructions to provision your Barracuda SSL VPN Vx appliance.

VMware Fusion 3.x

1. From the **File** menu, select **Open a Virtual Machine**.
2. Navigate to the **BarracudaSSLVPN.vmx** file.
3. Use the default settings, and click **Finish**.
4. Start the appliance.
5. Follow the [Quick Start Guide](#) instructions to provision your Barracuda SSL VPN Vx appliance.

Deploying XVA Images

Citrix XEN Server 5.5+

1. From the **File** menu in the XenCenter client, select **Import**.
2. Browse to the **BarracudaSSLVPN-<version#>-fw_FIRMWARE_-<version#>.xva** file, and click **Next**.
3. Follow the instructions to configure the **Storage** and **Networking** pages.
4. When prompted, review the template information and click **Finish** to import the template.
5. Right-click the resulting template, and select **New VM**.
6. Follow the [Quick Start Guide](#) instructions to provision your virtual appliance.

How to Enable Promiscuous Mode on VMware for the Barracuda Network Connector

If your virtual appliance is running on a VMware hypervisor, you must enable promiscuous mode on the appliance so that Barracuda Network Connector can work correctly.

About Promiscuous Mode

Place the virtual network adapter for the Barracuda SSL VPN Vx in promiscuous mode so that it can detect all frames that are passed on the virtual switch.

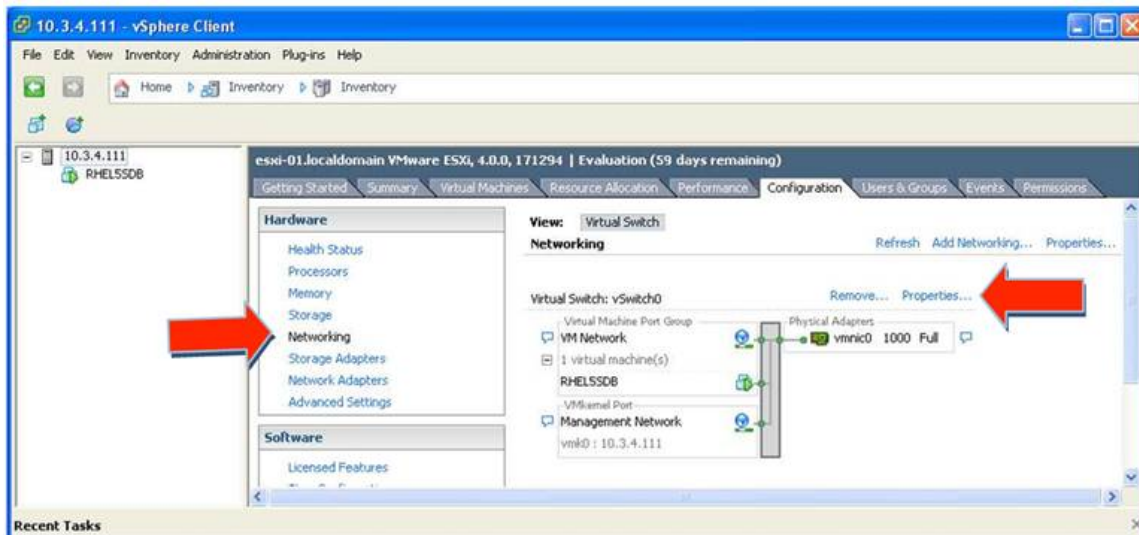
If you have already set up a Barracuda SSL VPN Vx system but did not enable promiscuous mode, you may see issues where the network connectivity seems intermittent. Experience suggests that the virtual interface does not receive all of the packets that it should. As a result,

Barracuda Networks recommends that you configure a port group to allow promiscuous mode.

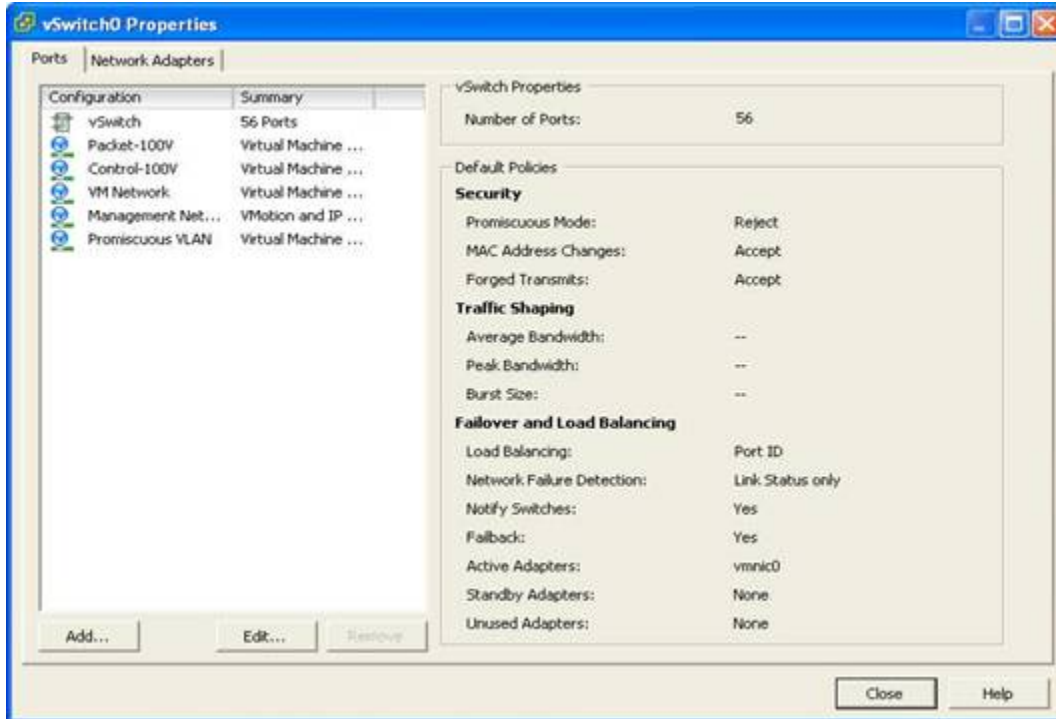
Enable Promiscuous Mode on a vSwitch

Add a new port group, and set it to promiscuous mode. Then set your VM client to the port group.

1. Log into the vSphere client, and select the ESX host.
2. Click the **Configuration** tab.
3. From the **Hardware** menu in the left pane, select **Networking**.
4. On the summary page for the virtual switch, click the **Properties** link.

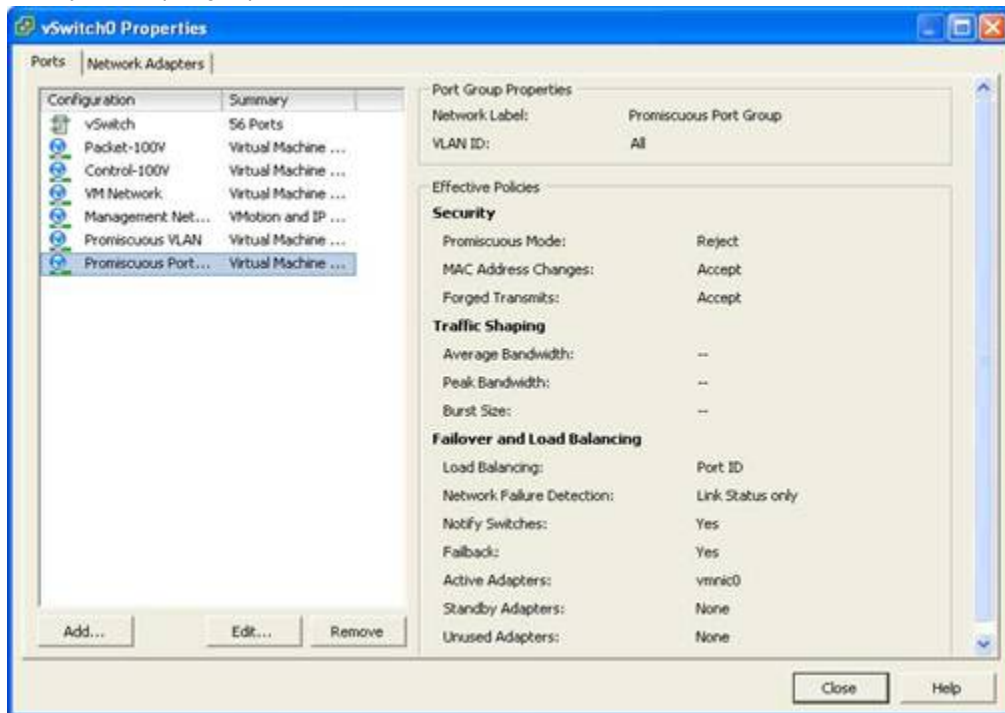


In the properties window that opens, you can modify the vSwitch configuration by port group. Under the **Ports** tab, virtual port groups are listed. Under the **Network Adapters** tab, physical network interface cards in the server are listed. To see a summary of a port group's settings, click its name. In the figure below, you can see that **Promiscuous Mode** is set to **Reject** (off).

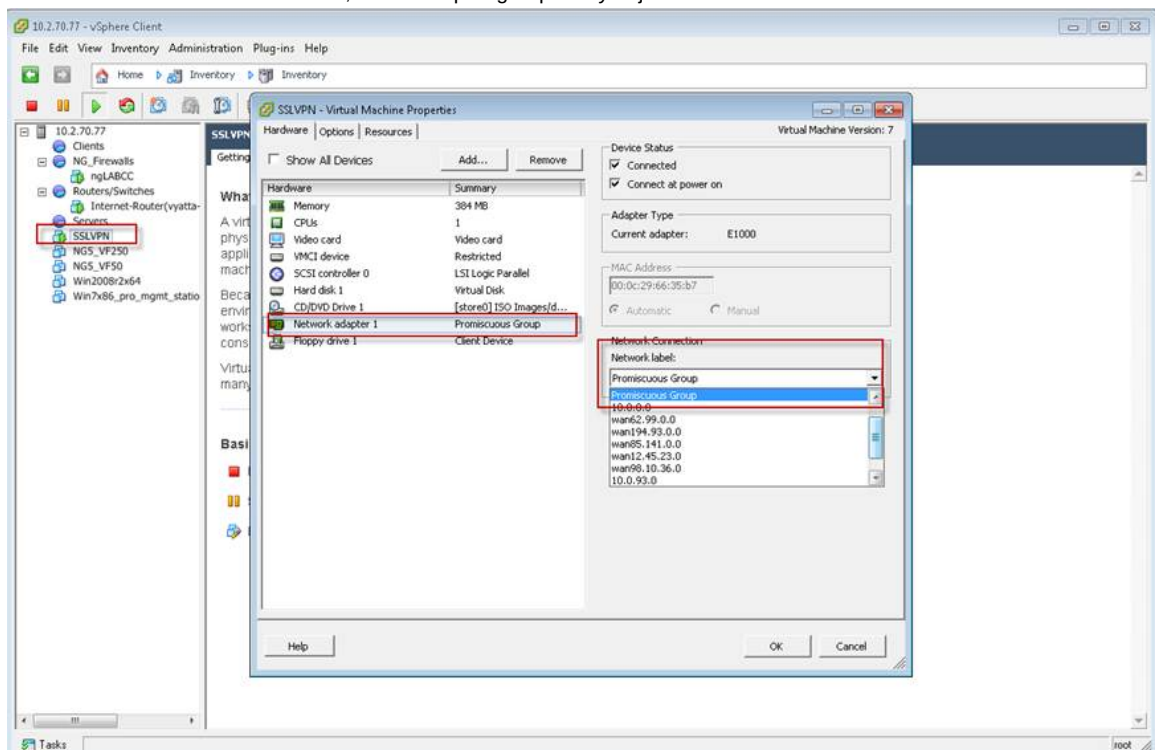


5. Add a port group.
 - a. Under the **Ports** tab, click **Add**.
 - b. Select **Virtual Machine**, and click **Next**.
 - c. Enter a **Network Label**, and set the **VLAN ID** to **4095** to enable trunking on the port group. This creates a VMware VLAN that lets the port group see the traffic on any VLAN without altering the VLAN tags.
 - d. Click **Finish**.

6. Set the port group to promiscuous mode.
 - a. Select your new port group, and click **Edit**.



- b. Click the **Security** tab.
 - c. From the **Promiscuous Mode** list, select **Accept**.
 - d. Click **OK**, and then click **Close**.
7. Set your VM client to the new port group.
 - a. Right-click the Barracuda SSL VPN virtual machine, and select **Edit Settings**.
 - b. In the left pane, click **Network Adapter 1**.
 - c. In the **Network Connection** section, select the port group that you just created and click **OK**.



Barracuda SSL VPN Vx Quick Start Guide

After your virtual appliance has been deployed, you must provision it. You need your

Barracuda Vx license token, which you received via email or from the website when you downloaded the Barracuda SSL VPN Vx package. The license token is a 15 character string, formatted like this: 01234-56789-ACEFG.

Complete the following steps:

- [Before You Begin](#)
- [Step 1. Enter the License Code](#)
- [Step 2. Open Firewall Ports](#)
- [Step 3. Log Into the Appliance Web Interface and Verify Configuration](#)
- [Step 4. Update the Firmware](#)
- [Step 5. Change the Administrator Password for the Appliance Web Interface](#)
- [Step 6. Route Incoming SSL Connections to the Barracuda SSL VPN Vx](#)
- [Step 7. Verify Incoming SSL Connections to the Barracuda SSL VPN Vx](#)
- [Next Step](#)

Related Articles
• Barracuda SSL VPN Administrative Interfaces • Backing Up Your Virtual Machine System State

Before You Begin

Deploy the Barracuda SSL VPN Vx on your hypervisor. For more information, see [How to Deploy Barracuda SSL VPN Vx Virtual Images](#).

Step 1. Enter the License Code

Enter the license token to start automatically downloading your license.

1. Start your virtual appliance.
2. Open the console for the Barracuda SSL VPN virtual machine.
3. When the login prompt appears, log in as admin with the password admin.
4. In the text-based menu, set the IP address and, under **Licensing**, enter your Barracuda license token and default domain to complete provisioning. The virtual machine reboots after you finish the configuration.

Step 2. Open Firewall Ports

If your Barracuda SSL VPN Vx is located behind a corporate firewall, open the following ports on your firewall to ensure proper operation:

Port	Protocol	Direction	Usage
22	TCP	Out	Remote diagnostics and service (recommended)
25	TCP	Out	Email alerts and one-time passwords
53	TCP/UDP	Out	DNS
80	TCP	Out	Energize Updates
123	UDP	Out	Network Time Protocol (NTP)
443	TCP	In/Out	HTTPS/SSL port for SSL VPN access
8000	TCP	In/Out	External appliance administrator port (HTTP)
8443	TCP	In/Out	External appliance administrator port (HTTPS)

If PPTP or L2TP/IPsec access is required, also open the following ports:

Port	Protocol	Direction	Usage
47	GRE	In/Out	PPTP
1723	TCP	In	PPTP
500	UDP	In	L2TP/IPsec
4500	UDP	In	L2TP/IPsec

Note: Only open the appliance administrator interface ports on 8000/8443 if you intend to manage the appliance from outside the corporate network.

Configure your network firewall to allow ICMP traffic to outside servers, and open port 443 to `updates.barracudacentral.com`. You must also verify that your DNS servers can resolve `updates.barracudacentral.com` from the Internet.

Step 3. Log Into the Appliance Web Interface and Verify Configuration

Log into the Barracuda SSL VPN Vx web interface, and finalize the configuration of the appliance.

1. In your browser, go to `https://<configured IP address for the Barracuda SSL VPN>:8443`.
2. Log into the Barracuda SSL VPN Vx web interface as the administrator:
Username: admin **Password:** admin
3. Go to the **BASIC > IP Configuration** page and verify that the following settings are correct:
 - **IP Address, Subnet Mask, and Default Gateway.**
 - **Primary DNS Server and Secondary DNS Server.**
 - (If you are using a proxy server on your network) **ProxyServer Configuration.**

Step 4. Update the Firmware

Go to the **ADVANCED > Firmware Update** page. If there is a new **Latest General Release** available, perform the following steps to update the system firmware:

1. Click **Download Now** next to the firmware version that you want to install.
2. When the download finishes, click **Apply Now** to install the firmware. The firmware installation takes a few minutes to complete.
After the firmware has been applied, the Barracuda SSL VPN Vx automatically reboots. The login page displays when the system has come back up.
3. Log back into the web interface, and read the Release Notes to learn about enhancements and new features.

For more information, see [Update Firmware](#).

Step 5. Change the Administrator Password for the Appliance Web Interface

To prevent unauthorized use, change the default administrator password to a more secure password. Go to the **BASIC > Administration** page, enter your old and new passwords, and then click **Save Password**. This only changes the password for the appliance web interface. The password for the `ssladmin` user on the SSL VPN web interface must be changed separately.

Step 6. Route Incoming SSL Connections to the Barracuda SSL VPN Vx

Route HTTPS incoming connections on port 443 to the virtual appliance. This is typically achieved by configuring your corporate firewall to port forward SSL connections directly to the Barracuda SSL VPN Vx.



Ports for Remote Appliance Management

If you are managing the virtual appliance from outside the corporate network, the appliance administrator web interface ports on 8000/8443 need similar port forward configurations. Barracuda Networks recommends that you use the appliance web interface on port 8443 (HTTPS).

Step 7. Verify Incoming SSL Connections to the Barracuda SSL VPN Vx

After you configure your corporate firewall to route SSL connections to the Barracuda SSL VPN Vx, verify that you can accept incoming SSL connections.

1. Test the connection by using a web browser from the Internet (not inside the LAN) to establish an SSL connection to the external IP address of your corporate firewall. For example, if your firewall's external IP address is 23.45.67.89, go to <https://23.45.67.89> in your browser.
2. When you are prompted to accept an untrusted SSL certificate, accept the warning and proceed to load the page.
If you see the Barracuda SSL VPN login screen, this confirms that your appliance can receive connections from the Internet.

Next Step

Configure your virtual machine. For instructions, see [Getting Started](#).

High Availability Deployment

High availability is available for the Barracuda SSL VPN 480 and above. Clustering two or three Barracuda SSL VPNs provides you with a high-availability, fault-tolerant environment that supports data redundancy and centralized policy management. After you configure one HA unit, configuration settings are synchronized across the cluster. You can cluster the Barracuda SSL VPN in two ways: simple high availability or high availability with a load balancer.

Simple High Availability

If you configure two or more Barracuda SSL VPNs in a high availability setup without a load balancer, configurations are synced between the units but only one unit processes traffic. The secondary unit is passive and monitors the health of the primary unit. If the active system becomes unavailable, the secondary unit takes over automatically.

For more information, see [How to Configure a High Availability Cluster](#).

High Availability with a Load Balancer

If you want all clustered Barracuda SSL VPNs to process traffic, use a load balancer (such as the Barracuda Load Balancer) to direct traffic to the HA units while maintaining session persistence. You must have a load balancer to spread the load over all Barracuda SSL VPN cluster members. It is recommended that you configure the Barracuda Load Balancer in Bridge-Path (recommended) or Route-Path mode.

To cluster your Barracuda SSL VPNs with a load balancer, complete the following tasks:

1. Configure the Barracuda Load Balancer. For instructions, see [Barracuda Load Balancer Bridge-Path Deployment](#) or [How to Set Up a Barracuda Load Balancer for Route-Path Deployment](#).
2. Configure Simple High Availability. See [How to Configure a High Availability Cluster](#).

How to Configure a High Availability Cluster

Follow these instructions to cluster your Barracuda SSL VPN systems. These instructions apply to both simple high-availability and for clustering with a load balancer.

In this article:

- [Before you Begin](#)
- [Adding an Appliance to the Cluster](#)
- [Simple High-Availability](#)
- [Creating a High-Availability Cluster](#)
- [Setting Non-Proxied Hosts](#)
- [Non-Clustered Data](#)

Related Articles

- [High Availability Deployment](#)
- [How to Update Firmware of Systems in a Cluster](#)

Before you Begin

Log in to the appliance interface using the admin account, and perform the following steps for **each** system that will be in the cluster:

1. Complete the installation process.
2. Make sure that each Barracuda SSL VPN are the same model. It is possible to mix hardware and virtual appliances.
3. Make sure that each Barracuda SSL VPN is on exactly the same firmware version using the **ADVANCED > Firmware** page.
4. Make sure that each Barracuda SSL VPN has the same time zone using the **BASIC > Administration** page.

5. Create a backup of the existing Barracuda SSL VPN configuration using the **ADVANCED > Backup** page.
6. Use the **ADVANCED > Task Manager** page to verify that no processes are running.
7. On this page, enter the **Cluster Shared Secret** and click **Save Changes**. This is the password shared by all Barracuda SSL VPN appliances in this cluster. It is limited to only ASCII characters.

Adding an Appliance to the Cluster

Any Barracuda SSL VPN appliance that is added to the cluster will have most of its local data (except user data and that specified in [Non-Clustered Data](#) overwritten with settings extracted from the cluster. The first system (the one identified first in the **Add System** field) is the source for the initial settings.

1. In the **Add System** field, enter the IP address of a system in the cluster (or, the first system if the cluster has not yet been created). A fully-qualified domain name can be entered, but could cause name resolution issues so is not recommended.
2. Click **Join Cluster**. The time to complete the join depends on the number of users, domains, and the load on each Barracuda SSL VPN appliance. During this time the configuration from the other system will be copied onto this system. The system will restart, and you will need to login and navigate to this page.
3. On each system in the cluster, perform the following:
 - a. Refresh the **ADVANCED > Linked Management** page to view the updated status.
 - b. Verify that the **Clustered Systems** list contains the IP address of *each* clustered system.
 - c. Verify that the **Connection Status** indicates that each clustered system is up and communicating with this system. The column displays green for each system that is available and red for each system that cannot be reached. Initially, it may take up to a minute for the status light to turn green. The **Synchronization Latency** field tells how long it takes to send updates to each of the other systems in the cluster. The value of this field should be 2 seconds or less. If it is greater, configuration changes may not be propagated correctly.
 - d. The **Mode** column in the Clustered Systems table should usually show all systems in the cluster as being active. If a system is in standby mode, changes to its configuration are not propagated to other systems in the cluster.
4. (Optional) Distribute the incoming SSL traffic to each Barracuda SSL VPN using a load balancer.

Simple High-Availability

Simple High-Availability (HA) can be used in cases where more than one Barracuda SSL VPN is available to create a failover cluster but a load balancer is not in use. Only one SSL VPN system will actively process traffic. The other system(s) will act as passive backup(s).

In an HA cluster, a virtual IP address is used to access the SSL VPN service. If the active system becomes unavailable, one of the passive systems in the cluster will become active and serve requests directed to the virtual IP address. You will use the individual IP addresses of the systems in the cluster for management. When the originally active SSL VPN appliance becomes available again, it will act as a passive backup.

Creating a High-Availability Cluster

Use the following steps to create a high-availability cluster.

- Complete the steps in the [Adding an Appliance to the Cluster](#) task above.
- In the **Simple High-Availability** section, enter the Virtual IP address.
- On the initially-active system, select the High-Availability Master option.

Setting Non-Proxied Hosts

If the Barracuda SSL VPN systems are using a proxy (**BASIC > IP Configuration**), then you must also configure non-proxy hosts in the Barracuda SSL VPN appliance interface on port 443. To do this, log onto each Barracuda SSL VPN appliance interface. From the **ADVANCED > Configuration > Proxies** page, make sure there is a non-proxied host entry for your IP range that the clustered systems are on (for example 192.168.0.*). Without this setting, data synchronization may not occur and your systems will not be truly clustered.

Non-Clustered Data

 Energize updates do not synchronize across systems in a cluster.

The following data is not propagated to each system in the cluster:

- **IP Address**, **Subnet Mask**, and **Default Gateway** (on the **BASIC > IP Configuration** page).
- **Primary DNS Server** and **Secondary DNS Server** (on the **BASIC > IP Configuration** page).
- Serial number (this will never change).
- **Hostname** (on the **BASIC > IP Configuration** page).
- All SSL information, including saved certificates (on the **BASIC > SSL Certificate** page).
- Any advanced IP configuration (models 600 and above, on the **ADVANCED > Advanced IP Configuration** page).

- Administrator password.
- **Cluster Shared Secret**, though this must be the same for the cluster to work properly (on the **ADVANCED > Linked Management** page).
- **Time Zone** (on the **BASIC > Administration** page).
- The appliance GUI and SSL VPN HTTP and HTTPS ports.
- Whether the latest release notes have been read.
- All customized branding (models 600 and above, on the **ADVANCED > Appearance** page).

Licensing



For more questions about your Barracuda SSL VPN license, contact your Barracuda Networks sales representative.

The Barracuda SSL VPN virtual and physical appliances both have different base licences. For both appliance types, add-on subscription licenses are also available.

In this article:

- [Hardware Licenses](#)
- [Vx Licenses](#)
- [Subscription-Based Licenses](#)
 - [Energize Updates](#)
 - [Instant Replacement](#)
 - [Premium Support](#)

Hardware Licenses

Hardware appliances are limited only by the performance of the appliance's hardware. There is no limit to how many users can concurrently connect to the appliance. To help you size the appliance, Barracuda Network provides a [recommended number of concurrent users](#). If you are using the appliance with more than the recommended number of users, its performance declines, but users can continue using it.

Vx Licenses

Virtual licenses are limited by the number of CPU cores that are licensed for the appliance model. There is no per user license. If you use your Barracuda SSL VPN Vx with more users than recommended, the performance of the appliance declines but no users are blocked. When your user base grows, you can upgrade the license and add additional cores to the virtual machine for increased performance.

Subscription-Based Licenses

The following subscription-based licenses are available:

Energize Updates

Energize Updates offer the latest firmware, application definition, and security updates for your system. It also includes standard technical support (24x5).

Instant Replacement

With Instant Replacement, a replacement for your Barracuda SSL VPN hardware ships within 1 day if your appliance fails. Every 4 years, your Barracuda SSL VPN is replaced by a new appliance with the latest hardware for your SSL VPN model. Standard technical support (24x7) is also included.

An active Energize Updates subscription is required for the Instant Replacement subscription.

Premium Support

Premium Support subscriptions offer the highest level of 24/7 technical support for mission critical environments. Barracuda Networks is committed to meeting the demands of these environments by providing a dedicated and highly-trained technical support team.

An active Energize Updates subscription is required for the Premium Support Subscription.

Getting Started

Follow the instructions in this guide after you complete the steps explained in the [Barracuda SSL VPN Quick Start Guide \(PDF\)](#) that shipped with your appliance.

In this article:

- [Before You Begin](#)
- [Step 1. Install the SSL Certificate](#)
 - [Step 1.1. \(Optional\) Generate a CSR Request](#)
 - [Step 1.2. Upload Signed Certificates](#)
- [Step 2. Configure System Contact and Alert Email Addresses](#)
- [Step 3. Change the Administrator's Password for the SSL VPN Web Interface](#)
- [Next Steps](#)

Related Articles
• Administrative Interfaces • Barracuda SSL VPN Quick Start Guide (PDF)

Before You Begin

- Install Java Runtime version 1.6 or above on your client computers.
- Register a full DNS name for the Barracuda SSL VPN (e.g., `sslvpn.example.com`).
- (Recommended) Purchase an SSL certificate signed by a trusted CA.

Step 1. Install the SSL Certificate

To prevent certificate errors whenever your users connect to the Barracuda SSL VPN, it is recommended that you install an SSL certificate signed by a trusted CA. You can generate the signing request directly on the Barracuda SSL VPN. Your SSL certificate must use the full DNS name (e.g., `sslvpn.example.com`) for the **Common Name** attribute.

Step 1.1. (Optional) Generate a CSR Request

To generate a CSR request:

1. Log into the [appliance web interface](#) (e.g., `https://sslvpn.example.com:8443`).
2. Go to the **BASIC > SSL Certificate** page.
3. From the **Certificate Type** list, select **Trusted (Signed by a trusted CA)**.
4. In the **Trusted (Signed by a trusted CA)** section, click **Edit Data**.
5. In the **CSR Generation** window, enter the full DNS name (e.g., `sslvpn.example.com`), enter the requested information about your organization, and then click **Save Changes**.
6. Click **Download CSR**.

You can now submit the CSR to your Certificate Authority.

Step 1.2. Upload Signed Certificates

When the certificates are uploaded to the Barracuda SSL VPN, the **Certificate Candidates** table displays the current status of the certificates. The **Status** column displays **OK** when all required certificates have been uploaded.

1. Log into the [appliance web interface](#) (e.g., `https://sslvpn.example.com:8443`).
2. Go to the **BASIC > SSL Certificate** page
3. From the **Certificate Type** list, select **Trusted (Signed by a trusted CA)**.
4. In the **Trusted (Signed by a trusted CA)** section, upload the certificates that you received from the CA in the following order:
 - a. Root CA certificate (PEM or PKCS12)
 - b. (Depending on your CA) Intermediate CA certificate (PEM or PKCS12)
 - c. SSL server certificate (PEM or PKCS12)
5. Click **Use**.
6. In the **Synchronize SSL** section, click **Synchronize**.

Your SSL certificate is now installed on both the appliance and the SSL VPN web interface. To avoid Java runtime certificate errors, use the full DNS name to connect to your Barracuda SSL VPN.

Step 2. Configure System Contact and Alert Email Addresses

Specify the email addresses of those who should receive notifications from the Barracuda SSL VPN and emails from Barracuda Central.

1. Log into the [appliance web interface](#) (e.g., <https://sslvpn.example.com:8443>).
2. Go to the **BASIC > Administration** page.
3. In the **Email Notification** section, enter the email addresses of those who should receive system alerts and security news and updates.
4. Click **Save Changes**.

Step 3. Change the Administrator's Password for the SSL VPN Web Interface

Change the password used by ssladmin to log into the SSL VPN web interface.

1. Log into the [SSL VPN web interface](#) (e.g., <https://sslvpn.example.com>) with the default username and password of ssladmin.
2. Click **Manage System**, and then go to the **ACCESS CONTROL > Accounts** page.
3. In the **Accounts** section, locate the ssladmin user and click **More**.
4. Select **Set Password**.
5. Enter the new password and click **Save**. The password must conform to the password rules defined for the appliance.

Next Steps

After you set up and explore the Barracuda SSL VPN, you can complete the following tasks:

Task	Articles
Configure a User Database.	• How to Create and Modify User Databases • Example - Create a User Database with Active Directory
Configure Authentication Schemes.	Authentication Schemes
Configure Policies.	How to Configure Policies
Configure Access Rights.	Access Rights
Configure Resources.	Resources
(Optional) Configure L2TP/IPsec or PPTP access.	• How to Configure IPsec • How to Configure PPTP

Administrative Interfaces

The Barracuda SSL VPN uses two administrative interfaces: the appliance web interface and the SSL VPN web interface.

Appliance Web Interface

You can access the appliance web interface at either of the following IP addresses:

<https://<configured IP address for the Barracuda SSL VPN>:8443> or <http://<configured IP address for the Barracuda SSL VPN>:8000>

This interface listens on port 8000 (HTTP) or 8443 (HTTPS). Log into this interface to configure all non-user facing options including network configuration, clustering, firmware upgrades, and Energize Updates. The default login credentials for the appliance web interface are:

- **User:** admin
- **Password:** admin

SSL VPN Web Interface

You can access the SSL VPN web interface at:

<https://<configured IP address for the Barracuda SSL VPN>>

This interface listens on port 443 (HTTPS). Log into this interface to configure all settings for the SSL VPN service. It also includes all user facing settings and functionalities. The SSL VPN web interface can be used in two modes. You can switch between both modes by clicking the link in the upper right of the web interface:

- **Manage System** – Manage VPN access to the system.
- **Manage Account** – Manage the account settings.

The default login credentials for the SSL VPN web interface are:

- **User:** ssladmin
- **Password:** ssladmin

Access Control

To access and use the resources provided by the Barracuda SSL VPN, a user must be able to authenticate. Additionally, the user's device must adhere to any configured network access control (NAC) policies. You can configure user authentication as either a single- or multi-factor process, using a combination of information stored in the authentication services and additional authentication procedures defined in the Barracuda SSL VPN. After users log in, the levels of access and privileges assigned to them on a per-resource basis are defined by the policies that you configured.

In this article:

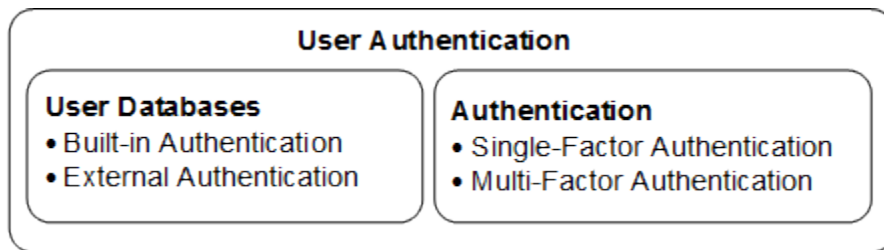
- [User Databases](#)
- [Authentication](#)
- [Policies](#)
- [Network Access Control \(NAC\)](#)

User Databases

Users and groups can be stored locally on the Barracuda SSL VPN's built-in user database or retrieved from external authentication servers. User databases define where user information is stored. The Barracuda SSL VPN 380 and above can use multiple user databases. You can configure every user database with global access rights and delegate some Super User responsibilities to management users in the user database.

For more information, see [How to Create and Modify User Databases](#).

Authentication

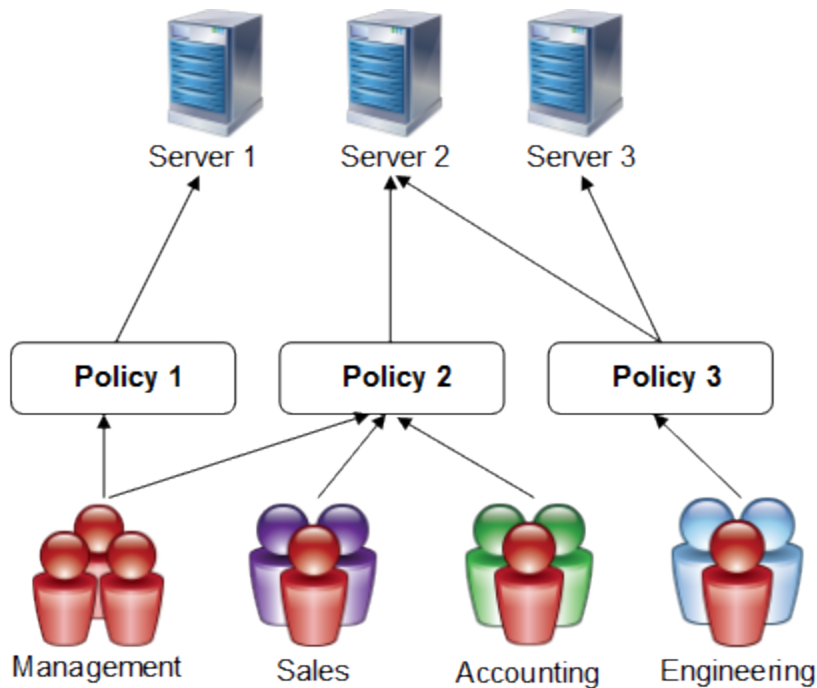


User authentication is not limited to password authentication. For greater security, the Barracuda SSL VPN provides multi-factor authentication. You can choose to activate a combination of the following authentication procedures:

- One-time passwords (sent via SMS or email)
- Authentication key
- Client certificates
- IP authentication
- PIN
- Security questions
- RADIUS
- Hardware token authentication (in combination with RADIUS or Client Certificates)

For more information on the available authentication schemes, see [Authentication Schemes](#).

Policies



Policies are lists of users and groups that are attached to resources. Users can only access a resource if they are included in the policy attached to the resource. A resource can include multiple policies that contain separate lists of users and groups. You can grant different users with varying levels of access to a resource by assigning Access Rights to the user or group. To help you easily assign resources to everybody, a built-in **Everyone** policy is included by default. You can delete the **Everyone** policy, locking out all users who do not have a specific Profile, Authentication Scheme, or Access Right assigned to them. It is recommended that you create policies for every distinct user group. For example, in a company with three departments, you can create separate policies for each department, management user, and administrator.

For more information on Policies, see [How to Configure Policies](#).

Network Access Control (NAC)

Network access control limits access to network resources, according to a variety of factors that are not connected to the user. Users who fail the NAC check are not allowed to log in until they have a conforming system. You can define exceptions for single users, so that they can continue using the service until they have time to update their system. User systems are evaluated by the following parameters:

- Time of day
- Operating system (type and if it is up-to-date)
- IP and MAC address
- Browser type and version
- Antivirus state (installed/up-to-date)
- Firewall
- Version of plugins installed
- Type of connection (Wi-Fi)
- Domain membership

To configure NAC, go to **Manage System > ACCESS CONTROL > NAC**. To define exceptions, go to **Manage System > ACCESS CONTROL > NAC Exceptions**.

How to Create and Modify User Databases

A user database specifies where user authentication information is stored. The Barracuda SSL VPN 380 and above support multiple user databases, letting you define different access policies for resources that are shared by users. The Barracuda SSL VPN supports authentication with the following services:

- [Active Directory](#)
- LDAP
- NIS
- OpenLDAP
- Built-in internal user database

Create the User Database

To create the user database:

1. Log into the [SSL VPN web interface](#).
2. Go to the **Manage System > ACCESS CONTROL > User Databases** page.
3. Enter a **Name** for the database.
4. In the **Create User Database** section, select and configure the authentication service.
5. Click **Add**.

The user database is now listed in the **User Database** section.

For more detailed information on how to create a user database with an external authentication service, see [Example - Create a User Database with Active Directory](#).

Delete the User Database

To delete a user database, go the **Manage System > ACCESS CONTROL > User Databases** page and click **Delete** next to the user database that you want to remove.

Modify the User Database

To modify a user database, go the **Manage System > ACCESS CONTROL > User Databases** page and click **Edit** next to the user database that you want to modify. You can now edit all settings for the user database. You can change authentication services for a user database; for example, you can switch to using Active Directory after using the built-in user database.

Example - Create a User Database with Active Directory

On the Barracuda SSL VPN, you can use an external Active Directory server for a user database. If you are using multiple user databases, on the Barracuda SSL VPN 380 or above, each user database manages its own authentication server configuration, so you can configure multiple Active Directory servers on the same unit.

Related Articles
• Access Control • How to Create and Modify User Databases

Before You Begin

Before you begin, verify that your Barracuda SSL VPN can reach your Microsoft Active Directory server. If you deployed your Barracuda SSL VPN in a DMZ, open the necessary ports for read or read/write access to your Active Directory server.

You also need the following information:

- Domain controller hostname
- Domain
- Service account name
- Service account password

Configure the User Database to Use an Active Directory Server

In the user database, provide the information required to connect with the Active Directory server.

1. Go to the **ACCESS CONTROL > User Databases** page.
2. In the **Create User Database** section, click the **Active Directory** tab.
3. In the **Connection** section, enter the following information:
 - **Domain Controller Hostname** – The name of the domain controller.
 - **Domain** – The domain.
 - **Service Account Name** – The user with permissions for read or read/write access to the Active Directory server. Write permissions must be configured in the Advanced Settings.
 - **Service Account Password** – The password for the user.
4. (Optional) Click **Show Advanced Settings** to configure Backup Domain Controller, SSL, read/write access, and OU Filters.
5. Click **Add**.

After you add the user database, it appears in the **User Databases** section on the bottom of the page.

Authentication Schemes

To authenticate users with more than just their usernames and passwords, configure authentication schemes. Every authentication scheme comprises at least one authentication module, such as PINs, passwords, certificates, or one-time-passwords. You can add as many authentication modules as your security policy requires. You can also configure a secure, default authentication method and offer users an alternative method to log in. For example, you can require users to use their hardware token with client certification for normal logins, but allow them to log in with a password and PIN code if they are using a computer that cannot use hardware tokens.

Some authentication modules must be used with other authentication modules. These modules are referred to as "secondary" authentication modules because they require user information. Some modules can be used as primary or secondary authentication modules. The following table lists the type of each available authentication module :

Authentication Module	Type
Client Certificate	Primary/Secondary
IP Address	Primary/Secondary
Password	Primary/Secondary
PIN	Primary/Secondary
Public Key	Primary/Secondary
RADIUS	Primary/Secondary
OTP (One-Time Passwords)	Secondary
Personal Questions	Secondary

Client Certificate

The Client Certificate module validates an SSL client certificate installed in the browser's certificate store against the root certificate that is uploaded to the Barracuda SSL VPN. The SSL client certificate can be installed manually, per Active Directory policy, or with a hardware token using the vendor's utility. It is recommended that you use the Client Certificate module as a secondary module, because it authenticates the browser and not the user directly. This is not the case when using hardware tokens or SSL client certificates containing user information that is checked when processing the login.

For more information, see [How to Configure SSL Client Certificate Authentication](#).

IP Address

The IP Address module is useful when users always log in from the same computer with the same IP address. You must manually specify the allowed IP address for every user. If a user tries to authenticate from a computer with a different IP address, the login attempt is denied.

To configure the IP Address module, go to the **ACCESS CONTROL > Accounts** page and specify the allowed IP address for each user. To let a user log in from any IP address, enter an asterisk (*).

Password

Password authentication is the classic authentication module and is used for almost every account. Passwords can be used either from external authentication sources, such as an Active Directory server, or from the built-in user database. You can define a password policy to ensure that only safe passwords are used. Passwords for external authentication methods can only be changed if the appliance has read/write access.

For more information on external authentication, see [How to Create and Modify User Databases](#).

PIN

A PIN is a numeric password. Its length is configurable and usually varies between four and six digits. You can let users create their PINs during initial logins, or you can manually assign PINs. After a PIN's configured lifetime, it expires and the user is asked to create a new PIN during the next login. To prevent weak PINs, disable the use of sequential numbers (e.g., 1234).

To configure the PIN module, go to the **PIN** section on the **ACCESS CONTROL > Security Settings** page.

Public Key

Public key authentication is one of the most secure methods of authentication, because the authentication information can be stored on a removable medium such as a USB key device. You can generate the key files for every user, or you can reset the public keys for everyone, letting users generate the keys during initial logins. After the key is generated, the login applet searches external media and the user's home directory for available keys. The user selects the correct key and enters the matching passphrase to complete the login.

For more information, see [How to Configure Public Key Authentication](#).

RADIUS

External RADIUS servers can be queried by the appliance to authenticate users. RADIUS servers are often used for external authentication methods that require users to enter a secondary challenge password.

RADIUS servers are also integrated with some hardware token solutions. The hardware token generates a login passphrase and the RADIUS server interfaces with the external security appliance from the hardware token vendor, validating the string from the hardware key generator. Challenge images can be used in combination with RADIUS authentication.

Because the RADIUS server is an external authentication service, it is not managed by the appliance. You must verify that the user information hosted on the RADIUS server corresponds to the information stored in the user database on the Barracuda SSL VPN.

For more information, see [Example - How to Install and Configure YubiRADIUS](#) and [Example - Authentication with SMS Passcode RADIUS server](#).

OTP (One-Time Password)

You can use one-time password (OTP) authentication as only a secondary authentication module. The OTP is generated by the appliance at login and is only valid for a short period of time. The OTP can be delivered by email or SMS (if an external SMTP to SMS service is available). If you do not want users to wait for OTPs during login, you can configure the appliance to deliver OTPs before login and set a longer expiration time (hours or days). If a user's OTP expires before it can be used, a new OTP is sent during the user's next login. External OTP systems (e.g., [SMS Passcode](#)) interface with the Barracuda SSL VPN via the RADIUS server and not with the OTP authentication module.

For more information, see [How to Configure One-Time Password \(OTP\) Authentication](#).

Personal Questions

You can use the Personal Questions module as only a secondary authentication module. It does not require any external servers or configuration. When users initially log in, they are asked five questions and their answers are stored by the module.

To authenticate a user, the module randomly selects one of the preconfigured questions and compares the user input to the stored answer. If the user input matches the answer, the user is logged in.

Hardware Token Authentication

Two factor or multi factor authentication is considered to be strong authentication, using a combination of the "something you know" and "something you have" principles. For the Barracuda SSL VPN these hardware solutions are based on two different authentication mechanisms, the RADIUS and the SSL Client Certificate authentication modules.

In this article:

- [Hardware Token Authentication using SSL Client Certificates](#)
- [Hardware Token Authentication using RADIUS Integration](#)
- [SafeNet iKey](#)
- [Aladdin eToken PRO](#)
- [RSA SecurID](#)
- [VASCO Digipass](#)
- [Secure Computing Safeword](#)

Related Articles

- [Authentication Schemes](#)
- [Example - How to Install and Configure YubiRADIUS](#)
- [SSL Client Certificate Authentication](#)

Hardware Token Authentication using SSL Client Certificates

The token or smart card contains an SSL client certificate which is used to authenticate to the system. Some vendors require software installed on the client, or card readers depending on the solution.

- SafeNet iKey 2032
- Aladdin eToken PRO

Hardware Token Authentication using RADIUS Integration

Other hardware token authentication servers use a built-in or external RADIUS server. The Barracuda SSL VPN queries the RADIUS server as a part of its multi factor authentication process. This way OTP and CryptoCard tokens can be used.

- RSA SecurID
- VASCO Digipass Token
- Secure Computing Safeword

SafeNet iKey

This product uses a small USB device typically carried on your key chain. It uses SSL client certificates to present a certificate to the Barracuda SSL VPN. The user also has to enter a secret pass phrase, further improving security. The client computer must have a special utility (CIP) installed, which uploads the certificate on the USB token to the windows certificate store. The browser then uses this certificate when authenticating to the Barracuda SSL VPN.

Aladdin eToken PRO

Similar to the SafeNet iKey the Aladdin eToken uses an SSL client certificate to authenticate. It also uses a special software, which has to be manually installed on every client computer.

RSA SecurID

RSA SecurID uses its built-in RADIUS server to enable communication between the appliance and the RSA server. In combination with an Active Directory user database this method is especially powerful as account management may be centrally managed with both the appliance and RSA Authentication Manager reading accounts from your Active Directory domain.

VASCO Digipass

A VASCO server can authenticate with the Barracuda SSL VPN via an external RADIUS server. The VASCO server currently does not include a RADIUS server.

Secure Computing Safeword

Safeword servers include a RADIUS feature that can be used to authenticate to the Barracuda SSL VPN. Note that Safeword requires an Active Directory database and Internet Authentication Server (IAS) installed on the Domain Controller.

How to Configure One-Time Password (OTP) Authentication

One-time passwords (OTPs) are passwords that can only be used once in a predefined time frame, usually just minutes. You can configure the Barracuda SSL VPN to send the OTP to users by either email or SMS. OTPs do not require any special hardware or infrastructure. Any device that receives email or SMS can be used to receive the OTP.

- To configure the Barracuda SSL VPN to send OTPs by email, configure the SMTP server and the OTP settings.
- To configure the Barracuda SSL VPN to send the OTPs by SMS, configure the SMTP server, the OTP settings, and an SMTP to SMS service.

Related Articles

- [Authentication Schemes](#)
- [Regular Expressions \(Reference\)](#)
- [Example - Authentication with SMS Passcode RADIUS server](#)

In this article:

- [Prerequisites for Sending OTPs by SMS](#)
- [Step 1. Configure the SMTP Server](#)
- [Step 2. Configure the OTP Settings](#)
- [Step 3. \(If Sending OTPs via SMS\) Configure the SMTP to SMS Service](#)

Prerequisites for Sending OTPs by SMS

If you want to send OTPs by SMS:

- You must have an account for an SMTP to SMS service that can send SMS to cell phones in your country
- Determine the address format for sending SMS over email. Each service provider uses a different format.
- Every user must have the `mobile.number` attribute set.

Step 1. Configure the SMTP Server

Configure the SMTP server that will be used to send the OTPs.

1. Select the user database that you want to configure the SMTP server for. To configure an SMTP server for all user databases, select **Global View**.
2. Go to the **Manage System > BASIC > Configuration** page.
3. In the **SMTP** section, enter the settings for your SMTP server.
4. Click **Save Changes**.

Step 2. Configure the OTP Settings

Specify when OTPs are sent, how they are sent, and what kind of OTPs are generated by the Barracuda SSL VPN.

1. Go to the **Manage System > ACCESS CONTROL > Security Settings** page.
2. In the **One-Time Password** section, configure the following settings:
 - **Send Mode** – Select **At Login** to send the OTP during user logins.
 - **Method of password delivery** – You can select either **Email** to send the OTP via email or **SMS over Email** to send the OTP to users' cell phones.
 - **Generation Type** – Select the type of OTP that you want the appliance to generate. If you experience problems with character encoding in your emails or SMS, select **ASCII**.
3. Click **Save Changes**.

If you configured the Barracuda SSL VPN to send OTPs by email, no additional configurations are required. When the appliance sends an OTP, it obtains the email address of the user from the user database.

Step 3. (If Sending OTPs via SMS) Configure the SMTP to SMS Service

If you configured the Barracuda SSL VPN to send the OTPs by SMS, provide the information required to connect with the SMTP to SMS service that you are using.

1. Open the **Manage System > ACCESS CONTROL > Configuration** page.
2. In the **SMS** section, enter the following information, depending on the requirements of your SMTP to SMS service provider:
 - **SMS Gateway Address** – The email address for the SMS gateway. A common example would be: `${userAttributes.mobileNumber}@example.com`
 - **SMS Provider Credentials** – Usually the credentials and the text are entered here.
3. Click **Save Changes**.

How to Configure Public Key Authentication

The public key authentication module is a very secure authentication mechanism, combining a client certificate and a passphrase with the possibility to store the authentication keys on an external storage device. No external services or appliances are needed, all keys are generated

and managed by the Barracuda SSL VPN. The module can be used as primary or secondary authentication mechanism. The administrator has to generate a private and public key which is then uploaded to the Barracuda SSL VPN and stored on the users USB key device or home directory. When you authenticate with a public key, the following steps are followed:

1. The Barracuda SSL VPN generates a random ticket (certificate)
2. The user selects the private key and enters the corresponding passphrase.
3. The ticket is signed with the users private key and sent to the Barracuda SSL VPN.
4. The Barracuda SSL VPN uses checks if the signed ticket is valid with its public key.
5. If the check was successful, the user is logged in.

In this article:

- [Step 1. Create or Modify the Authentication Scheme](#)
- [Step 2. Configure Key Authentication Settings](#)
- [Step 3. Generate Keys](#)
 - [Creation and Distribution by Administrator](#)
 - [Creation by Users on Login](#)

Step 1. Create or Modify the Authentication Scheme

To use the public key authentication create or modify the authentication scheme and add the **Public Key Authentication** module to the configuration. If you want users to generate their own initial public keys, the public key authentication module will query the users password to authenticate them before generating the new keys.

Step 2. Configure Key Authentication Settings

Configure the key authentication module:

1. Open the **Manage System > RESOURCES > Security Settings** page.
2. In the **Key Authentication** section, configure the following settings:
 - **Allow user to create initial authentication key**
 - **Enforce Password Security Policy**

Step 3. Generate Keys

There are two ways the keys can be generated:

Creation and Distribution by Administrator

The administrator can initialize the key for a user:

1. Open the **Manage System > ACCESS CONTROL > Accounts** page.
2. Click on the **More** link for the user you want to generate the key for.
3. Select **Generate Authentication Key**.
4. Enter the **Passphrase**. The Administrator can require the passphrase to conform to the password security policy.
5. Click **Generate**.
6. Download the zip file..
7. Click **Close**.
8. Distribute the key stored in the zip file to the individual user. Barracuda Networks recommends using a USB key for greater security.

Creation by Users on Login

The administrator can also reset the Authentication key, forcing the user to generate a new key at the next login. The user must enter his system password when generating the new key.

1. Open the **Manage System > ACCESS CONTROL > Accounts** page.
2. In the **Accounts** section, locate the individual user who should create the authentication key and click **More**.
3. Select **Reset Authentication Key**.

On the next log in the user will be asked to enter his password and a new passphrase. The Barracuda SSL VPN will then generate a zip file containing the authentication key, which the user can download.

How to Configure SSL Client Certificate Authentication

SSL client certificates are a very secure secondary authentication method. When this feature is enabled, users can provide an SSL client certificate, but it is not required by the server. During users' initial login, they must install the SSL client certificate into the certificate store of the

browser or operating system. After the initial setup is complete, the authentication process requires minimal user interaction. Users must only select the installed certificate when prompted, and the rest of the setup is completed automatically by the browser and the Barracuda SSL VPN.

The Barracuda SSL VPN validates the offered client certificate according to parameters that are defined by you. If you do not check for certificate attributes that are unique to each user, any user can log in with a browser that has a valid SSL client certificate. To prevent this, you must always combine SSL client certificate authentication with another authentication method like a password prompt.

In this article:

- [Before You Begin](#)
- [Step 1. Upload the Root Certificate](#)
- [Step 2. Configure Client Certificate Authentication Settings](#)
- [Step 3. Add the Client Certificate Authentication Module to an Authentication Scheme](#)

Before You Begin

Create the following:

- A root certificate.
- Client certificates.
- An authentication scheme using client certificates as a primary or secondary authentication method.

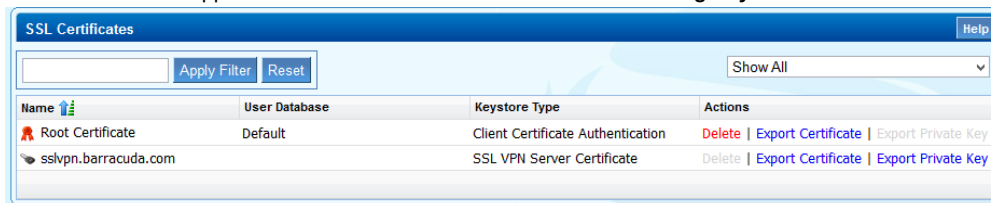
For more information on creating your own self-signed root certificates, see [How to Create Certificates with XCA](#).

Step 1. Upload the Root Certificate

For every user database, you can create or upload a unique root certificate.

1. Open the **Manage System > ADVANCED > SSL Certificates** page.
2. In the **Import Key Type** section, select **A root Certificate Authority certificate you trust for client certificate authentication** from the **Certificate Type** list
3. In the **Import Details** section, select the user database that you want to upload the root certificate to.
4. Click **Browse**, and select the root certificate file. The certificate file must have a cer or crt extension.
5. Click **Save**.

The certificate then appears in the **SSL Certificates** section on the **Manage System > ADVANCED > SSL Certificates** page.



Name	User Database	Keystore Type	Actions
Root Certificate	Default	Client Certificate Authentication	Delete Export Certificate Export Private Key
sslvpn.barracuda.com		SSL VPN Server Certificate	Delete Export Certificate Export Private Key

Step 2. Configure Client Certificate Authentication Settings

Configure the settings for the client certificates.

1. Log into the [SSL VPN web interface](#).
2. Go to the **Manage System > ACCESS CONTROL > Security Settings** page.
3. In the **Client Certificates** section, configure the client certificates settings.
4. Click **Save Changes**.

Step 3. Add the Client Certificate Authentication Module to an Authentication Scheme

1. Log into the [SSL VPN web interface](#).
2. Go to the **Manage System > ACCESS CONTROL > Authentication Schemes** page.
3. **Edit** an authentication scheme.
4. Double-click **Client Certificate** to add the authentication module.
5. Click **Save**.

Example - How to Install and Configure YubiRADIUS

This article provides step-by-step instructions on how to deploy the YubiRADIUS virtual appliance in context with Barracuda SSL VPN. Once YubiRADIUS is installed, Barracuda SSL VPN can be configured to act as a RADIUS client.

In this article:

- [Pre-Requisites](#)
- [Reference](#)
- [Installing the YubiRADIUS Virtual Appliance](#)
- [Configuring the YubiRADIUS Virtual Appliance](#)
- [Configuring Barracuda SSL VPN](#)

Pre-Requisites

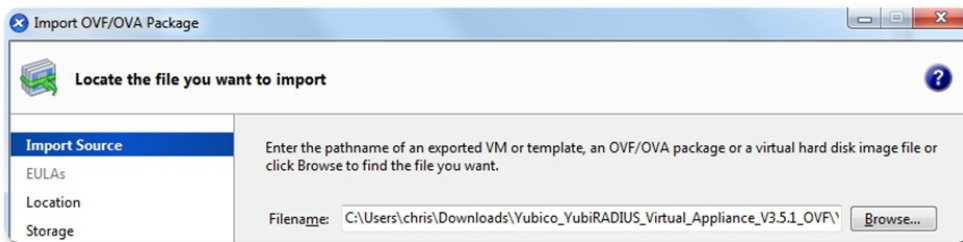
- A YubiKey
- A VM host server to load the Virtual Appliance
- An external user database, such as Active Directory or LDAP, that both Barracuda SSL VPN and YubiRADIUS servers can query

Reference

The YubiRADIUS configuration guide can be found here: http://static.yubico.com/var/uploads/pdfs/YubiRADIUS_Virtual_Appliance_3_5_1.pdf.

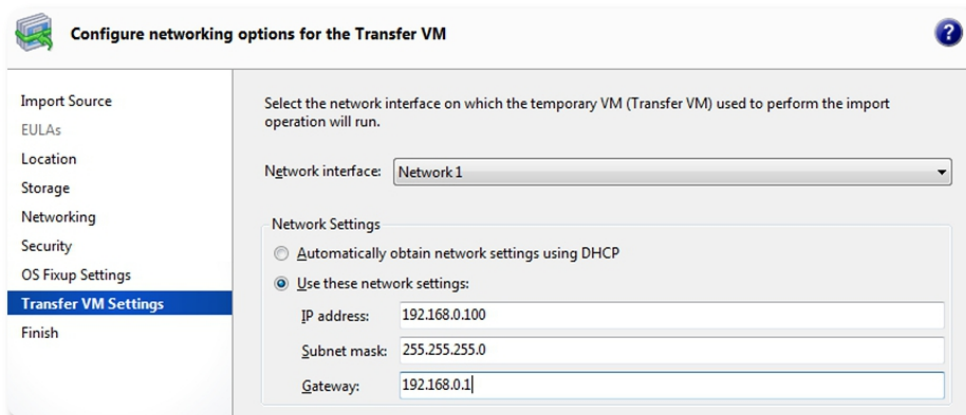
Installing the YubiRADIUS Virtual Appliance

1. Go to <http://www.yubico.com/yubiradius>.
2. You will need to register on the yubico website to download the virtual appliance image: enter your registration details and click **Submit**. Yubico will send an email containing a link to the image.
3. Click the link to download the image. Extract the files and import the virtual machine into your VM host server (The images show XenServer).



4. The default settings should be correct in most cases, apart from the network settings, where it might be required to set a static address (unless IP reservations will be used on the DHCP server).

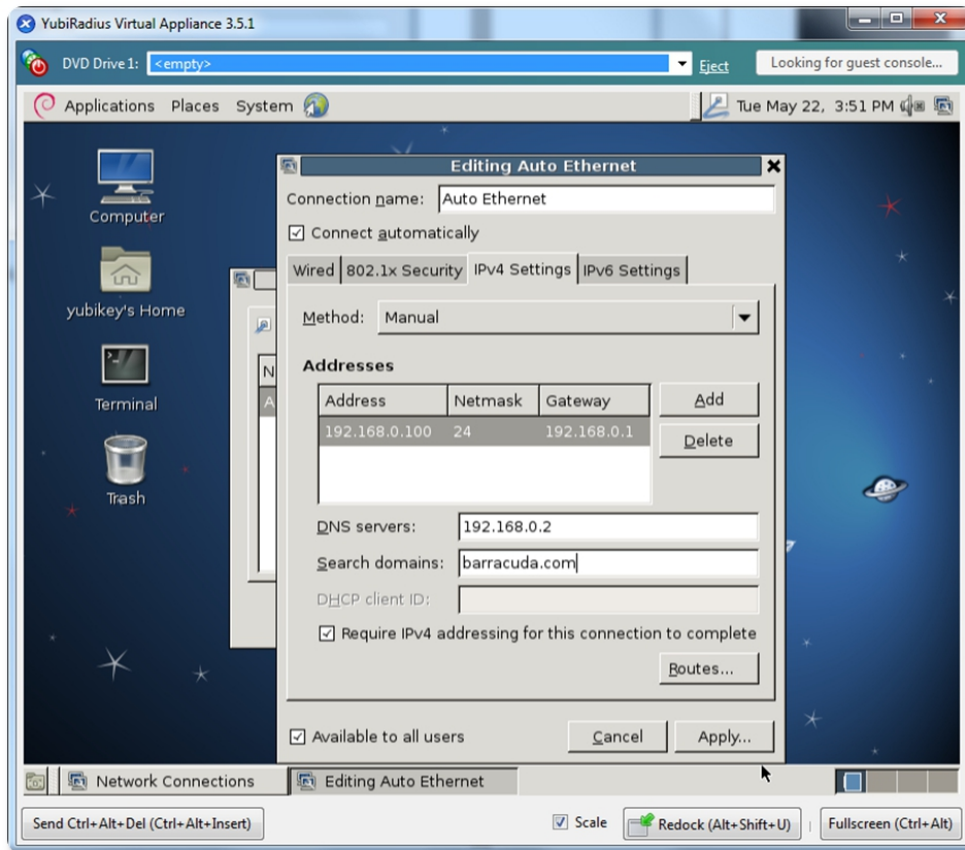
 If entering a static IP address does not work at this time, log in to the appliance after the import process has finished, and set the IP address then.



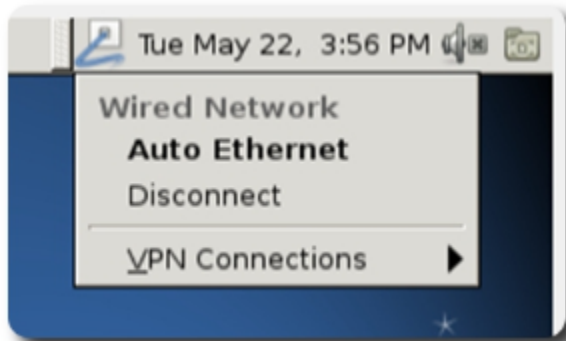
Configuring the YubiRADIUS Virtual Appliance

1. After the virtual appliance has been imported, start it and connect to the console. Log in as user: **yubikey** with the password: **yubico**.
2. Check the networking by clicking the **System** menu > **Preferences** > **Network Connections**.
3. Select **Auto Ethernet** and click **Edit**. Select the **IPv4** tab and change the settings as required by adding a static address (it is important also to set the DNS here, otherwise connections to the user database may fail).

4. Apply the settings and enter the user password to confirm.



5. Disconnect from the network and reconnect using the network icon in the top right area of the screen.



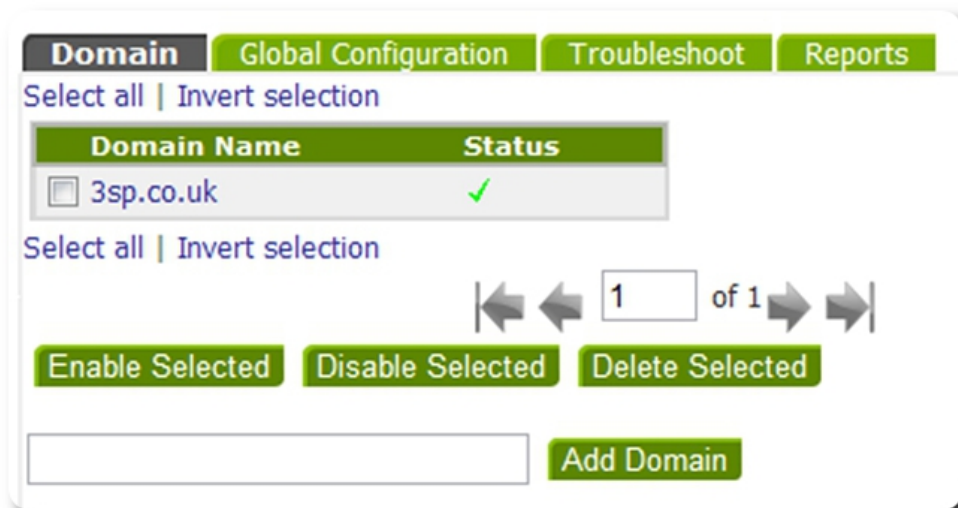
6. With a web browser, navigate to the IP address of the appliance, which should present a Webmin login screen.



7. Log in with user **yubikey** and password **yubico**.



8. Enter a valid domain name and click **Add Domain**.



9. Click on the **Global Configuration** tab, then click **General**. You may opt to set **Auto-provisioning** to **Yes**, although it may be simpler to keep it set to **No** initially. Ensure that **Append OTP to** is set to **Password**.

General Configuration

Enable Auto-provisioning

☐ Yes ☒ No

Enable Auto-provisioning for multiple YubiKeys

☐ Yes ☒ No

On service fail, fallback to single factor?

☒ Yes ☐ No

Append OTP to

☐ Username ☒ Password

Temporary token length

Enable YubiApp registration

☐ Yes ☒ No

On service fail, send email alert?

☐ Yes ☒ No

Selecting "Yes" will send an email alert if OTP validation server is unavailable.

Email Address(es)

Save

10. Go back to **Global Configuration** and click **Validation Server**. This configuration will use the YubiCloud validation servers. For this to work, your network's firewall needs to allow outbound access on TCP ports 80 and 443 to *api.yubico.com*, *api2.yubico.com*, *api3.yubico.com*, *api4.yubico.com* and *api5.yubico.com*.

Validation Server Configuration

Validation Server

☒ YubiCloud - Online Validation Service
☐ Local validation Server on YubiRADIUS Virtual Appliance
☐ Other (for example:
"http://192.168.1.1/wsapi/2.0/verify")

Client ID

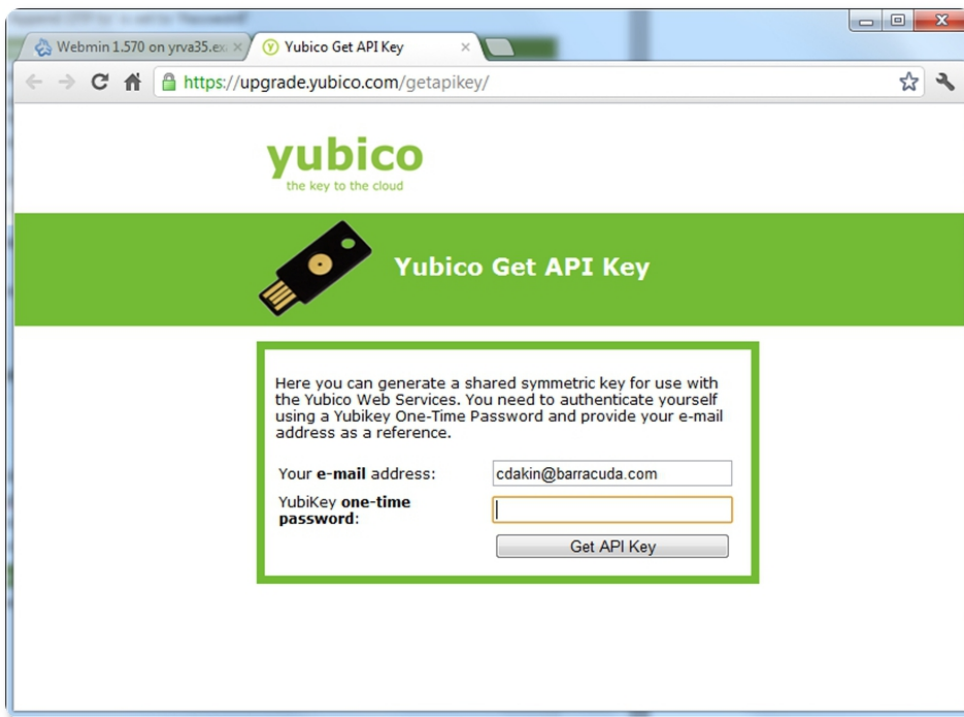
☐ Show API Key

API Key

Confirm API Key

Save

11. To get a client ID and API key, go to <https://upgrade.yubico.com/getapikey/>. Enter the email address you used to register with Yubico. Select the password field, insert your YubiKey and press the button to add the password.



12. Insert the resulting client ID and secret key in the **Client ID** and **API key** fields and click **Save**.

13. Navigate to the **Domain** tab, then select your domain that was added earlier.

14. Click the **Users Import** tab. Enter the hostname for your user database and set the **Directory Type** to either **Active Directory** or **LDAP**.

- Set the **Base DN** to the LDAP-style root DN.
- Enter the username that should be used to connect and cache the users in DN format.
- Enter the service password.
- Set the schedule for how often YubiRADIUS should re-cache the list of users (hourly is recommended).

If you wish to only import users of a certain group, use a filter like this example in Active Directory: (memberOf=<full DN of group>) e.g CN=Group,OU=myOU,DC=domain,DC=com(objectClass=person) - which could be used to import all users. Enter the identifier of the username. For Active Directory, this will be SAMAccountName, for OpenLDAP it is normally uid.

15. Click **Save**, then click **Import users**.

Users/Groups
Users Import
Configuration

User Import Configuration Management

This section is used for importing users for the selected domain from an organization's LDAP/AD server periodically or manually.

Use Secure Connection?
☐ Yes
☒ No

LDAP/AD Server Address or Host Name

Backup LDAP/AD Server Address or Host Name (optional; for user authentication only)

Port (use 0 or blank to use the default port)

Directory Type

LDAP Version

Base DN

User DN

Password

Schedule

Timeout (Seconds)

Filter

Notes

Login Name Identifier

Save
Import Users

The users should now be imported successfully:

User Import Configuration Management

User Import operation started...
Connecting to LDAP/AD server.
Successfully connected to LDAP/AD server.
Binding to server with given user credentials.
Successfully bound to server.
Searching user records.
User records found.
Added new users.
Disabled deleted users.
Successfully updated users records.
Connecting to LDAP/AD server.
Importing users from LDAP/AD..... (This may take a while depending on your directory size)
User Import operation completed...

- Now go back to the **Domain** tab and click on your domain, you should now see which accounts may authenticate. If you click on a group, the users should become visible (note that there are currently no YubiKeys assigned).

Users/Groups

Users Import

Configuration

Select all

Invert selection

Create a new user

Assign a new YubiKey

Temporary token settings

Username	Login Name	YubiKey ID	User DN	Temp. Token Status	Directory Status	YubiKey Status
☐	Further Test Accounts	No YubiKey Assigned	OU=Further Test Accounts,OU=Test Accounts,DC=3sp,DC=co,DC=uk	✗	✓	✗
☐	Redirected profile folders	No YubiKey Assigned	OU=Redirected profile folders,OU=Test Accounts,DC=3sp,DC=co,DC=uk	✗	✓	✗
☐ test&	tesr&	No YubiKey Assigned	CN=test&,OU=Test Accounts,DC=3sp,DC=co,DC=uk	✗	✓	✗
☐ test	test	No YubiKey Assigned	CN=test,OU=Test Accounts,DC=3sp,DC=co,DC=uk	✗	✓	✗
☐	Test Group	No YubiKey Assigned	CN=Test Group,OU=Test Accounts,DC=3sp,DC=co,DC=uk	✗	✓	✗
☐	TestOU	No YubiKey Assigned	OU=TestOU,OU=Test Accounts,DC=3sp,DC=co,DC=uk	✗	✓	✗
☐ user.dot	user.dot	No YubiKey Assigned	CN=user.dot,OU=Test Accounts,DC=3sp,DC=co,DC=uk	✗	✓	✗

Select all

Invert selection

Create a new user

Assign a new YubiKey

Temporary token settings

◀◀

1

of 1

▶▶

Enable YubiKey

Disable YubiKey

Unassign YubiKey

Delete User

- Click the **Assign a new YubiKey** link at the bottom of the page. Enter the username you wish to assign a key to, select the OTP box and press the **YubiKey** button to send the password.

User Details

Login Name

YubiKey OTP

Create

- Your user should now have a YubiKey ID assigned as shown in the example below:

☐	test&	test&	No YubiKey Assigned	CN=test&,OU=Test Accounts,DC=3sp,DC=co,DC=uk	✗	✓
☒	test	test	No YubiKey Assigned	CN=test,OU=Test Accounts,DC=3sp,DC=co,DC=uk	✗	✓
☐	test()	test()	No YubiKey Assigned	CN=test(),OU=Test Accounts,DC=3sp,DC=co,DC=uk	✗	✓

- At this point a local test can be performed. Go back to the main **YubiRADIUS Virtual Appliance** module under **Servers** in the left menu and click the **Troubleshoot** tab.

- Keep the **Client Secret** as: **test**
- Enter the username that has the YubiKey assigned.
- Enter the user's database password.
- Click the **OTP field** and press the **YubiKey** button.

This should authenticate successfully.

Domain

Global Configuration

Troubleshoot

Reports

RadTest

This page allows you to test the YubiRADIUS Virtual Appliance setup by querying it directly with requests.

Client Secret (shared encryption key; default=test)

test

Username

test

Password

YubiKey OTP or Temporary Token

Send Request

Reset

RadTest Response: **Successful!**

```

Sending Access-Request of id 8 to 127.0.0.1 port 1812
  User-Name = "test"
  User-Password = "password123?ccccccbgigfdhfgchfrhjcderrfucnerhdbnbgucennu"
  NAS-IP-Address = 127.0.0.1
  NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=8, length=20

```

- The final appliance configuration step is to inform the system that the Barracuda SSL VPN will be a RADIUS client:

- Access the **Domain** tab, then select your domain.

- Click the **Configuration** tab.
- In the **Add Client** section, enter the IP address of the Barracuda SSL VPN, and set and confirm a shared secret (this will be needed for the Barracuda SSL VPN configuration).
- Click **Add**.

Add Client

The client administrator of RADIUS Service can configure its RADIUS Client IP address and shared secret for security of RADIUS messages. Please note, RADIUS Service uses UDP port 1812 for communication.

Client IP (e.g. 192.168.0.0/24)

Client Secret (shared encryption key)

Confirm Client Secret

Add

The RADIUS client should now appear in the list:

Client IP	Created	Status
☐ 10.14.0.19	2012-05-22 18:29:27	✓
Select all Invert selection		

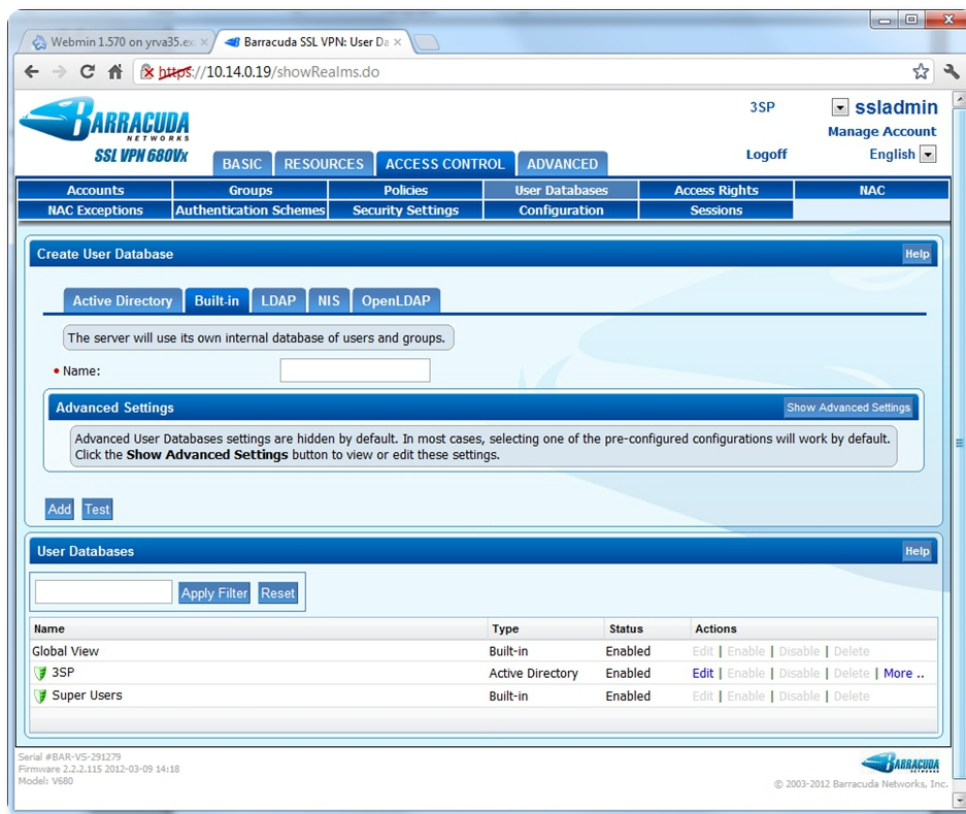
Configuring Barracuda SSL VPN

1. Log on to the Barracuda SSL VPN web interface as `ssladmin` and navigate to **ACCESS CONTROL > Authentication Schemes**. Create a new authentication scheme which contains the RADIUS module (Select **RADIUS**, click **Add**). Select a policy which will be able to use this authentication (such as *Everyone* for example) and click **Add**. The new module will appear, this may be set as the default module by clicking **More..** next to the item and choosing **Increase Priority** until it appears at the top of the list.

The screenshot shows the Barracuda SSL VPN web interface. The top navigation bar includes 'BASIC', 'RESOURCES', 'ACCESS CONTROL', and 'ADVANCED'. Under 'ACCESS CONTROL', there are sub-tabs: 'Accounts', 'Groups', 'Policies', 'User Databases', 'Access Rights', and 'IAC'. The 'Authentication Schemes' sub-tab is selected. The 'Create Authentication Scheme' section has a 'Name' field and two lists: 'Available modules' (containing Authentication Key, Client Certificate, IP Authentication, One-Time Password (Secondary), and Password) and 'Available Policies' (containing Admin Rights, Administrators, Barracuda, Customers, and Employees). There are 'Add >>', '<< Remove', 'Up', and 'Down' buttons between the lists. Below these are 'Selected modules' and 'Selected Policies' lists. An 'Add' button is at the bottom of the 'Create Authentication Scheme' section. The 'Authentication Schemes' section shows a table with the following data:

Name	Actions
☒ RADIUS	Edit Copy Delete More ..
☒ Password	Edit Copy Delete More ..
☒ WebDAV	Edit Copy Delete

2. Navigate to **ACCESS CONTROL > User Databases** and ensure you are connected to the same user database that YubiRADIUS is connected to. If not, edit the user database and change the settings accordingly.



3. Navigate to **ACCESS CONTROL > Configuration** and scroll to the **RADIUS** section.
 - a. Enter the hostname or IP address for the YubiRADIUS appliance in the **RADIUS Server** field.
 - b. Keep the ports the same.
 - c. Enter the same shared secret as used in the YubiRADIUS RADIUS client configuration earlier.
 - d. Set the **Authentication Method** to **PAP**.
Everything else may use the default settings.
 - e. Click **Save Changes**.

The screenshot shows the 'RADIUS' configuration page in the Barracuda SSL VPN Webmin interface. The page is titled 'RADIUS' and has a 'Save Changes' button in the top right corner. The configuration fields are as follows:

- RADIUS Server:** 10.14.4.48
- Backup RADIUS Servers:** A list of backup servers with 'Add >>' and '<< Remove' buttons. A note says 'Host names of backup RADIUS Servers.'
- Authentication Port:** 1812. A note states: 'This is the port number stipulated for the RADIUS authentication process. It **MUST** be a valid integer port between 0 and 65535. Default (1812).'
- Accounting Port:** 1813. A note states: 'This is the port number stipulated for the RADIUS accounting process. It **MUST** be a valid integer port between 0 and 65535. Default (1813).'
- Shared Secret:** A masked field (dots). A note says: 'The RADIUS shared secret which has been set up on the RADIUS server.'
- Authentication Method:** PAP. A note says: 'If your server does not use a specific authentication method, this value is ignored. The only methods that are currently supported in this configuration are PAP, CHAP, MSCHAP and MSCHAPv2.'
- Time Out:** 5. A note says: 'The timeout for a RADIUS message.'
- Authentication Retries:** 1. A note says: 'The number of retries for a RADIUS message.'
- RADIUS Attributes:** A list of attributes with 'Add >>' and '<< Remove' buttons. The current attributes are:
 - NAS-IP-Address=10.14.0.19
 - User-Name = %USERNAME%
 - User-Password = %PASSWORD%
 A note says: 'The RADIUS attributes required to execute the request.'
- Username Case:** Radio buttons for 'As Entered' (selected), 'Force Upper Case', and 'Force Lower Case'. A note says: 'Setting that defines what case the username is sent to the RADIUS server. Options are to leave as entered, force to upper case or force to lower case.'
- Password Prompt Text:** RADIUS Password. A note says: 'Customize the RADIUS password prompt text.'
- Reject Challenge:** Radio buttons for 'Yes' and 'No' (selected). A note says: 'Reject a challenge-response request from the RADIUS server. Default (true)'.
- Challenge Image URL:** A text field. A note says: 'A URL for generated challenge images. Leave blank to disable.'
- Allow Untrusted Challenge Image URL:** Radio buttons for 'Yes' and 'No' (selected). A note says: 'Allow Challenge Images to be server from untrusted servers.'

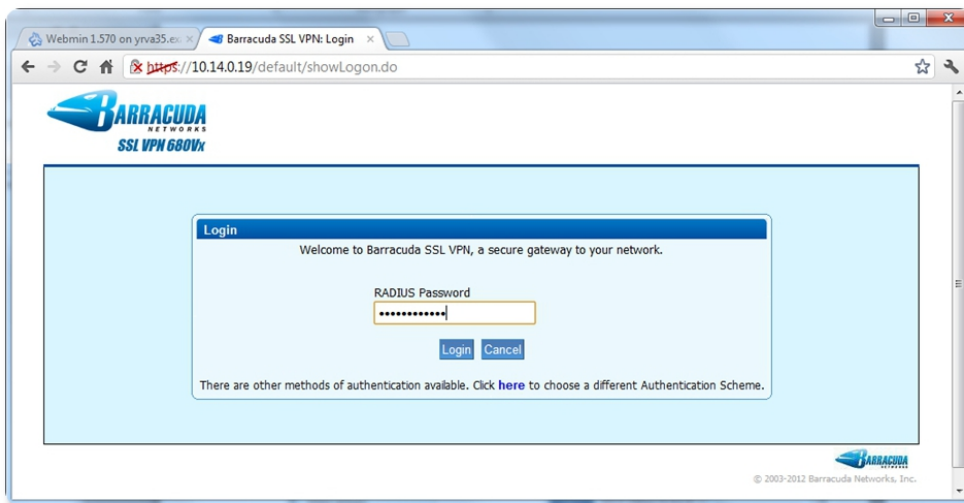
4. Now you can connect to the Barracuda SSL VPN via this user account. Enter the username and click **Login**.

The screenshot shows the 'Barracuda SSL VPN Login' page. The page has the Barracuda Networks logo and the text 'SSL VPN 6800x'. The login form is titled 'Login' and includes the following elements:

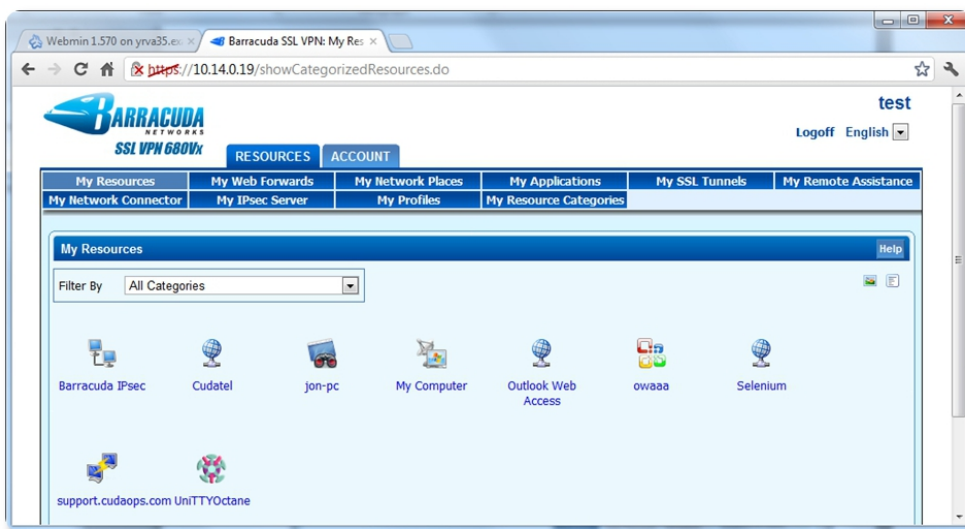
- A welcome message: 'Welcome to the Barracuda SSL VPN, a secure gateway to your network.'
- A 'Language' dropdown menu set to 'English'.
- A 'Username' text field containing the text 'test'.
- A 'Login' button.

At the bottom right, there is a copyright notice: '© 2003-2012 Barracuda Networks, Inc.'

5. Insert the user's database password (don't confirm with enter at this stage) and immediately press the **YubiKey** button (so that the password is a combination of the user's password + the YubiKey password).



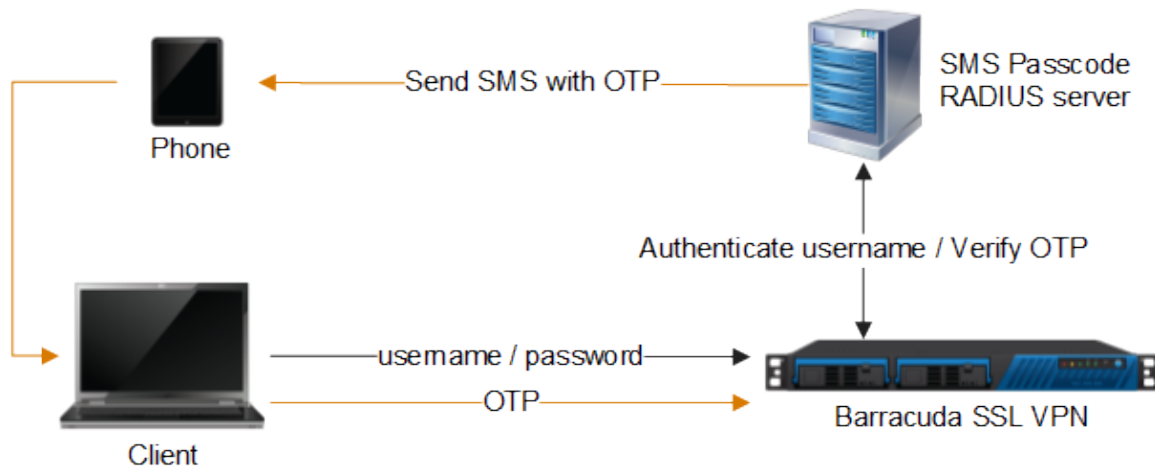
The user should now be logged on successfully:



Example - Authentication with SMS Passcode RADIUS server

You can use SMS Passcode servers to authenticate users with one-time passwords (OTP) that are sent via SMS. The user logs in with a username and password and then receives an SMS containing the OTP (e.g., nc43sa). After entering the OTP, the user is logged in. For multi-factor authentication, you can combine SMS Passcode with other authentication modules.

To set up authentication with SMS Passcode, configure a RADIUS server to be used by it and then create an authentication scheme that includes the RADIUS server.



In this article:

- Step 1. Configure the RADIUS Server
- Step 2. Create an Authentication Scheme
- Step 3. Test the SMS Passcode Authentication

Step 1. Configure the RADIUS Server

On the Barracuda SSL VPN, enter the configuration for the SMS Passcode RADIUS server.

1. Go to the **Manage System > ACCESS CONTROL > Configuration** page.
2. In the **RADIUS** section, enter the following information:
 - **RADIUS Server** – Enter the hostname or IP address of the SMS Passcode server.
 - **Authentication Port** – Enter 1812.
 - **Shared Secret** – Enter the shared secret. This passphrase must be configured on the SMS Passcode server.
 - **Authentication Method** – Select **PAP**.
 - **Reject Challenge** – Select **No**.
3. Click **Save Changes**.

RADIUS

Save Changes Help

RADIUS Server:

sms-radius.srv.local

Backup RADIUS Servers:

Hostname

Add >>

<< Remove

Hostnames

Host names of backup RADIUS Servers.

Authentication Port:

1812

This is the port number stipulated for the RADIUS authentication process. It **MUST** be a valid integer port between 0 and 65535. Default (1812).

Accounting Port:

1813

This is the port number stipulated for the RADIUS accounting process. It **MUST** be a valid integer port between 0 and 65535. Default (1813).

Shared Secret:

.....

The RADIUS shared secret which has been set up on the RADIUS server.

Authentication Method:

PAP

If your server does not use a specific authentication method, this value is ignored. The only methods that are currently supported in this configuration are **PAP**, **CHAP**, **MSCHAP** and **MSCHAPv2**.

Time Out:

30

The timeout for a RADIUS message.

Authentication Retries:

2

The number of retries for a RADIUS message.

RADIUS Attributes:

Attribute

\$()

Add >>

<< Remove

Attributes

NAS-IP-Address = \${radius:r
User-Name = \${session:use
User-Password = \${session:

The RADIUS attributes required to execute the request.

Username Case:

☒ As Entered
☐ Force Upper Case
☐ Force Lower Case

Setting that defines what case the username is sent to the RADIUS server. Options are to leave as entered, force to upper case or force to lower case.

Password Prompt Text:

RADIUS Password

Customize the RADIUS password prompt text.

Reject Challenge:

☐ Yes
☒ No

Reject a challenge-response request from the RADIUS server. Default (true)

Challenge Image URL:

A URL for generated challenge images. Leave blank to disable.

Allow Untrusted Challenge Image URL:

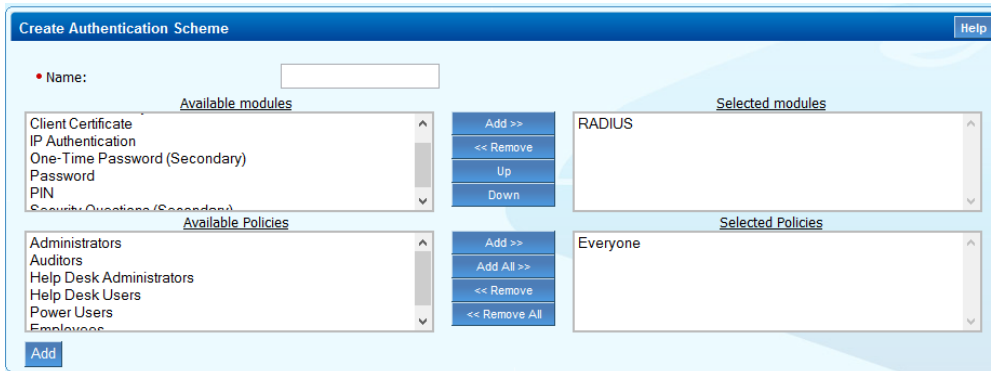
☐ Yes
☒ No

Allow Challenge Images to be server from untrusted servers.

Step 2. Create an Authentication Scheme

Create an authentication scheme that includes the SMS Passcode RADIUS server.

1. Go to the **Manage System > ACCESS CONTROL > Authentication Schemes** page.
2. In the **Create Authentication Scheme** section:
 - a. Enter a **Name** for the scheme (e.g., SMS Passcode RADIUS).
 - b. From the **Available modules** list, select **RADIUS** and click **Add**. RADIUS then appears in the **Selected modules** list.
 - c. (Optional) If additional authentication modules are required by your security policy, add them to the **Selected modules** list.
 - d. From the **Available Policies** list, select the policies that you want to apply this authentication scheme to and click **Add**. The policies then appear in the **Selected Policies** list.
 - e. Click **Add**.
3. (Optional) If you want to make the SMS Passcode authentication scheme the default, click the **More** link next to it in the **Authentication Schemes** section and then click **Increase Priority**.



Step 3. Test the SMS Passcode Authentication

To test the SMS Passcode authentication:

1. If the SMS Passcode authentication scheme is not the default scheme, select it.
 2. Enter your username.
 3. When prompted, enter your SMS Passcode password, and then click **Login**.
 4. After you receive the OTP via SMS, enter the OTP in the **Enter PASSCODE** field, and then click **Login**.
- You are now logged into your Barracuda SSL VPN.

How to Configure Policies

Policies are lists of users and groups with optional time and date restrictions. Users can only access a resource if their policy is attached to the resource. Every resource must have at least one policy attached.

When users log into the Barracuda SSL VPN, they can only view resources for which they meet the following policy criteria:

- They are listed in one or more of the policies that are attached to the resource.
- They are a member of a group listed in one or more of the policies that are attached to the resource.
- They are accessing the resource within the limits of the time and date restrictions that are set in the resource policies.
- Access method.

Related Articles
• Resources • Access Control

Create a Policy

Configure a set of access policies to meet your remote access needs.

1. Log into the [SSL VPN web interface](#).
2. In the upper right, verify that you have selected the correct user database.

3. Go to the **Manage System > ACCESS CONTROL > Policies** page.
4. In the **Create Policy** section, configure your policies. For each policy:
 - a. Enter a name for the policy.
 - b. Add the **Accounts** and **Groups** that must be members of the policy. The **Accounts** that you add appear in the **Selected Accounts** section, and the **Groups** that you add appear in the **Selected Groups** section.
 - c. Click **Add** to create the policy. The policy appears in the **Policies** section.

Edit a Policy

To change the membership and network access settings for a policy, go to the **Manage System > ACCESS CONTROL > Policies** page and click **Edit** next to the policy name.

To change the rights associated with a policy, go to the **Manage System > ACCESS CONTROL > Access Rights** page. For more information, see [Access Rights](#).

Access Rights

Access rights grant various permissions to configure resources and system settings. As administrator, you can assign access rights to individual users or groups (e.g., all team leaders). You can also use access rights to create administrators for all or just one user database. Access rights are classified as:

- **Resource Rights** – Lets users create, edit, and delete resources such as access rights, profiles, and network places.
- **System Rights** – Lets users create, edit, and delete system resources such as policies, SSL certificates, authentication schemes, account, and reporting.
- **Personal Rights** – Lets users manage personal resources in the Manage Account mode of the SSL VPN web interface.

You can create an access right for a single user database, or you can create an access right that is available to all user databases. You can also copy access rights between user databases.

In this article:

- [Create Access Rights](#)
- [Edit Access Rights](#)
- [Copy Access Rights to a Different User Database](#)

Create Access Rights

To create an access right:

1. Log into the [SSL VPN web interface](#).
2. Go to the **Manage System > ACCESS CONTROL > Access Rights** page.
3. In the **Create Access Rights** section, select the user database that you want to create the access right for. For example, if you want to create the access right for all user databases, select **Global View**.
4. Select the **Type** of access right that you are creating.
5. Enter a descriptive **Name** for the access right.
6. From the **Available Rights** list, select the rights that you want to add.
7. From the **Available Policies** list, select the policies that you want to assign the access rights for.
8. Click **Add**.

The new access right appears in the **Access Rights** section.

Edit Access Rights

To edit an access right, go to the **Manage System > ACCESS CONTROL > Access Rights** page and click **Edit** next to the name of the access right.

To remove an access right, click **Delete** next to the name of the access right.

Copy Access Rights to a Different User Database

To copy an access right to a different user database:

1. Log into the [SSL VPN web interface](#).
2. Open the **Manage System > ACCESS CONTROL > Access Rights** page.
3. In the **Access Rights** section, click **More** next to the name of the access right and select **Copy to User Database**.

4. In the **Copy to User Database** section of the **Edit Access Right** window, double-click the user databases that you want to copy the access right to.
5. Click **Save**.

Resources

Within the Barracuda SSL VPN, you can configure different types of internal network corporate resources that your users can access externally such as applications, email, network shares, or intranet websites. Within a resource, you can apply the policies that you have created. When users log into the Barracuda SSL VPN, their **RESOURCES** tab only lists the items to which they have been granted access by the system administrator.

For more information on the types of resources that you can configure on your Barracuda SSL VPN, see the articles that are linked in the following table:

Resource Type	Description	Link
Web Forwards	Access to intranet websites and internal web-based applications.	Web Forwards
Applications	Predefined and custom client/server applications within the secured network.	Applications
Network Connector	Full TCP/IP access into the secured network.	Network Connector
Network Places	Network shares on the internal network.	Network Places
SSL Tunnels	Create SSL tunnels to secure unencrypted intranet services.	SSL Tunnels

Web Forwards

To make web-based applications and internal websites accessible to remote users with the proper credentials, configure Web Forwards. With Web Forwards, sensitive information does not need to be placed outside of your corporate firewall. Because all communication is secured with SSL, additional encryption or authentication routines are not required for the site.

The type of Web Forward that you use depends on the directory structure of your internal websites. For the most popular web-based applications, you can use predefined templates to configure the Web Forward. For all other websites, you can configure custom Web Forwards.

Web Forward Templates

The Barracuda SSL VPN offers predefined Web Forward templates for the following types of applications and websites:

- **Development Tools** - E.g., JIRA 4.
- **Mail** - E.g., Outlook Web Access (see [How to Configure a Microsoft Exchange OWA Web Forward](#)).
- **Portals** - E.g., SharePoint (see [How to Configure a Microsoft SharePoint Web Forward](#)).
- **Terminal Services** - E.g., XenDesktop 5, RDP Clients.

Creating a Custom Web Forward

If none of the available Web Forward templates matches your requirements, you can create custom Web Forwards.

For more information, see [Custom Web Forwards](#) and [How to Create Custom Web Forwards](#).

In this Section

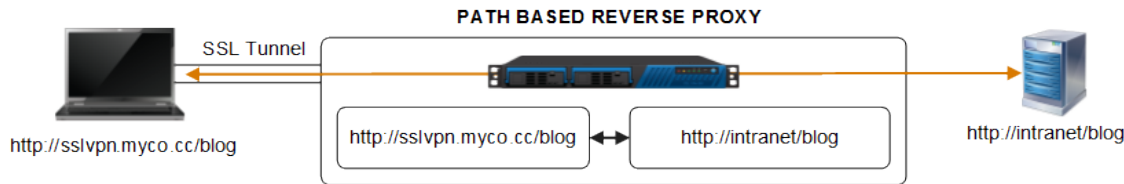
- [Custom Web Forwards](#)
- [How to Configure a Microsoft SharePoint Web Forward](#)
- [How to Configure a Microsoft Exchange OWA Web Forward](#)

Custom Web Forwards

To create a Web Forward for a intranet site or web-based application, for which there is no predefined template, you have to create a Custom Web Forward. The Barracuda SSL VPN can differentiate between these types of Web Forwards:

- Path-Based Reverse Proxy
- Host-Based Reverse Proxy
- Tunneled Proxy
- Replacement Proxy
- Direct URL

Path-Based Reverse Proxy



The Path-Based Reverse Proxy (most commonly used) acts as the front end to your web servers on the Internet or intranet. The Barracuda SSL VPN receives all the incoming web traffic from an external location and forwards it to the appropriate website host. For this proxy type to work, all possible destinations on the specified website or application for a particular Web Forward Resource must be within a directory on the web server - example: for Microsoft Outlook Web Access (OWA), */exchange* and */exchweb*.

This type of forward does not modify the data stream. The proxy works by matching unique paths in the request URI with the configured Web Forwards. For example, if you have a website that is accessible from the URL *http://intranet/blog* in your network you can configure the reverse proxy Web Forward with a path of */blog* so that all requests to the SSL VPN server URL *https://sslvpn.myco.cc/blog* are proxied to the destination site.

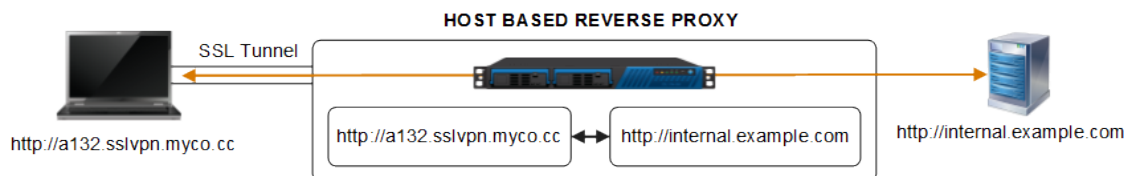
With a Path-Based Reverse Proxy, the Barracuda SSL VPN attempts to automatically detect all the paths that the target website uses, and add them to the Web Forward configuration when the Resource is launched. For example, when you create a Web Forward for *http://sslvpn.myco.cc/blog* and this blog page also contains images from a path called */images* from the root of the server, the Barracuda SSL VPN adds */blog* and */images* to the Web Forward configuration. This allows anything in the */blog* or */images* directory or subdirectories to work with this Web Forward. The following example shows the paths that the Barracuda SSL VPN added to the Web Forward *http://sslvpn.myco.cc/blog* which the user can access:

- *https://sslvpn.example.com/blog/images/picture.jpg* - The subdirectory of */images* below */blog* is added to this Web Forward.
- *https://sslvpn.example.com/blog/page2.htm* - *page.2.htm*, a child of */blog*, is added to this Web Forward.

When you try to access this Web Forward and the web content attempts to bring up an HTTP request that is not at one of those locations, such as: *http://sslvpn.example.local/news/index.html*, the Barracuda SSL VPN automatically adds the path specified by that request; in this case: */news*. Adding paths automatically does not work when they conflict with a path that the Barracuda SSL VPN uses to display HTTP content, such as */default* */theme* */js* */fs*. If parts of the web page are missing, the Barracuda SSL VPN might not have detected some of the paths. To resolve this issue, edit the Web Forward, and manually add these extra paths.

 To use the Path-Based Reverse Proxy, make sure that you set the **Always Launch Agent** option to Yes.

Host-Based Reverse Proxy



A host-based reverse proxy works in a similar way to a path-based reverse proxy, but is not restricted to subdirectories. However, the host must resolve properly via DNS. The proxy allows the web content to be located anywhere on the destination web server, including its root. This is useful for websites and applications that specify a host header or use relative paths in the content.

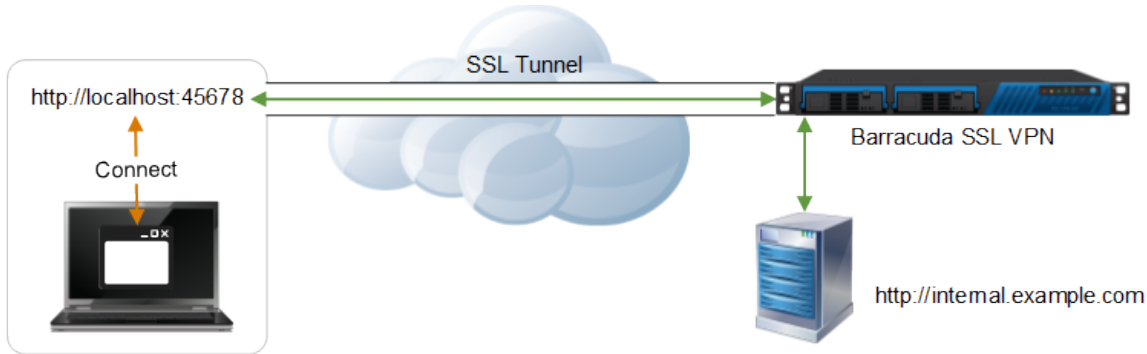
The Host-Based Reverse Proxy creates a unique hostname and appends it to the subdomain of the Barracuda SSL VPN.

For example: If the Barracuda SSL VPN hostname is *sslvpn.myco.cc*, the URL for the host-based reverse proxy Web Forward would be *https://<random string>.sslvpn.myco.cc*. Because a unique subdomain is created for each Web Forward configured as a Host-Based Reverse Proxy, you must configure a DNS entry on your DNS server for each subdomain that is used to resolve to the Barracuda SSL VPN. You can identify every

generated hostname and create an explicit entry for it on your DNS server, or create a wildcard entry so that all lookups resolve to the same IP address as the Barracuda SSL VPN. As with the Path-Based Reverse Proxy, accessing links to a location that was not specified in the configuration fails unless you configure the destination hostname as an allowed host (with the *Allowed Host* option).

i You must create configure your DNS server to resolve all generated subdomains to the IP address of the Barracuda SSL VPN.

Tunneled Proxy



A tunneled proxy uses the Barracuda SSL VPN Agent on the client to open up a SSL tunnel to the Barracuda SSL VPN. The clients browser connects to a localhost address (e.g., `http://localhost:45678`). A direct connection to the resource located behind the SSL VPN is then established through the SSL tunnel. This type of Custom Web Forward does not modify the data stream, but will only work as long as all links stay on the same destination host. If the destination site uses multiple domains, or sub-domains, a host file or a proxy auto-configuration file (PAC) with routing information can tell the client which additional target sites have to be routed through the SSL tunnel. If needed, the PAC file is downloaded to the remote system when the session is initiated.

The tunnel proxy the following basic configurations, based on your web resource:

- **None** - (Recommended at first use) Creates a simple SSL tunnel. The browser connects to a local address (e.g., `http://127.0.0.1:45678`). The SSL VPN Agent forwards all traffic from the localhost address through the SSL tunnel, where the connection with the configured destination host is made. Use the None proxy type for simple, static websites, that are not virtually hosted and do not check the headers for the hostname.
- **Host File Redirect** - Adds temporary entries to the remote system's host file to enable direct routing to the destination site. Upon launch of a Web Forward of this type, the Barracuda SSL VPN automatically uploads the additional configuration information to the remote system. Because of this, the user must have write permissions to the system's *hosts* file. This proxy type is typically used with Microsoft Silverlight applications, because they do not operate in a reverse proxy environment. The Host File Redirect proxy type only works with Windows applications and does not support single sign-on.
- **Proxy** - For complex environments, you can use the Proxy type to create a SSL Tunnel to a proxy server located in the destination network. This proxy type injects a proxy auto configuration (PAC) file into the browser with instructions about how to connect to different sites. These instructions redirect the target web requests through the tunnel. Use the Proxy proxy type when:
 - Laptop users do not need to disable their proxy settings when they are outside their corporate network.
 - Internal applications are hosted across WAN links. For example, if your users are in Austria but the Citrix server is hosted in the United States. You can use a PAC file to direct specific URLs to proxy servers that handles Citrix traffic exclusively. The rest of the traffic goes through your default Internet proxy in Austria.

i With Tunneled proxy, all the links must be relative on the host that you have defined. For example: `/folder/file.html` instead of `http://server/folder/file.html`

Replacement Proxy

A replacement proxy is generally used if all the other Custom Web Forward types cannot be used. This proxy type attempts to find all links in the website code and replace them with links pointing back to the Barracuda SSL VPN. The content of the web page is modified as it

passes through the SSL VPN, making it possible to create custom replacement values for different remote users.

If you have absolute URL addressing, use the Replacement Proxy when the other Custom Web Forward types do not work. The Replacement Proxy works most of the time, provided that the web page is not using a lot of JavaScript. However, using a Replacement Proxy is more resource intensive than the other proxies. Due to the number of ways it is possible to create links (in many different languages), this proxy type is not always successful. However, it is possible to create custom replacement values to get a website working through a replacement proxy Web Forward.

Direct URL

The Direct URL type is a direct link to an external website. Traffic does not pass through the Barracuda SSL VPN. This should be used for linking to external resources, like for example search engines, Wikipedia, etc...

How to Create Custom Web Forwards

The easiest way to create a Web Forward is by using one of the predefined templates, which include the most commonly used web applications. If your web application is not listed, create a custom Web Forward. You can configure the following types of custom Web Forwards:

- Path-Based Reverse Proxy
- Host-Based Reverse Proxy
- Tunneled Proxy
- Replacement Proxy
- Direct URL

If you do not know what type of Web Forward to use, Barracuda Networks recommends that you first try using the path-based reverse proxy. Note also that only one Web Forward can be launched with the same path. For more information on the available custom Web Forward types, see [Custom Web Forwards](#).

You can also edit the settings for the custom Web Forward to configure additional options such as its authentication type or allowed hosts.

After you finish configure the Web Forward, launch it to make it accessible to users.

In this article:

- [Step 1. Create the Web Forward](#)
- [Step 2. Edit the Web Forward](#)
- [Step 3. Launch the Web Forward](#)

Related Articles

- [Web Forwards](#)
- [Custom Web Forwards](#)

Step 1. Create the Web Forward

To create the custom Web Forward:

1. Log into the [SSL VPN web interface](#).
2. Go to the **Manage System > RESOURCES > Web Forwards** page.
3. In the upper right, verify that you have selected the correct user database.
4. In the **Create Web Forward** section:
 - a. Enter a name for the custom Web Forward. This name is displayed to end users.
 - b. From the **Web Forward Category** list, select the **Custom** check box. Then select the type of custom Web Forward that you are creating.
 - c. Configure the settings that appear for the custom Web Forward type that you selected.
 - d. Add the policies that you want to apply to the Web Forward.
5. Click **Add** to create the Web Forward. The new Web Forward appears in the **Web Forwards** section.

Step 2. Edit the Web Forward

To configure additional options (e.g., **Authentication Type** and **Allowed Hosts**) for the custom Web Forward, edit its settings.

1. In the **Web Forwards** section, click **Edit** next to the Web Forward entry.
2. In the **Edit Web Forward** window, configure the additional settings.
3. Click **Save**.

Step 3. Launch the Web Forward

Add a resource category to the Web Forward to make it available to users on their **My Resources** page.

1. In the **Web Forwards** section, click **Edit** next to the Web Forward entry.
2. In the **Edit Web Forward** window, scroll to the **Resource Categories** section, and add the available categories that you want to apply to the Web Forward.
3. If you want the Web Forward to automatically launch whenever users log into the Barracuda SSL VPN, scroll to the **Details** section and enable **Auto-Launch**.
4. Click **Save**.

How to Configure a Microsoft SharePoint Web Forward

When you create a Web Forward for SharePoint 2013 on the Barracuda SSL VPN, use the SharePoint 2013 template as described in the following configuration steps. To get SharePoint working through a proxy, you must also add **Alternate Access Mappings** to tell SharePoint to expect requests that were made to other hosts (namely, the Barracuda SSL VPN).

In this article:

- [Step 1. Configure SharePoint Server](#)
 - [Step 1a. Add Alternate Access Mappings](#)
 - [Step 1b. Restart the IIS Server](#)
- [Step 2. Create a Web Forward](#)

Related Articles

- [Web Forwards](#)
- [Custom Web Forwards](#)

Step 1. Configure SharePoint Server

To configure the settings for SharePoint, go to the SharePoint 2013 Central Administration console (this might be set up on <your SharePoint server>:1317). If it is not available, then, on the system that IIS is running on, navigate to **Start > SharePoint 2013 Central Administration** and complete the following steps:

Step 1a. Add Alternate Access Mappings

1. On the **Central Administration** page, click **Configure alternate access mappings** in the **System Settings** section.
2. Click **Edit Public URLs**.
3. Select *SharePoint - 80* from the **Alternate Access Mapping Collection** drop-down list.
4. Add the following entries:
 - **Default** - http://<your SharePoint server>
 - **Intranet** - http://<your fully qualified SharePoint server>
 - **Internet** - http://<your fully qualified Barracuda SSL VPN>
 - **Extranet** - https://<your fully qualified Barracuda SSL VPN>

Step 1b. Restart the IIS Server

1. Go to **Start > Internet Information Services (IIS) Manager**.
2. In the left hand pane, click **SHAREPOINT**.
3. In the right hand pane under **Manage Server**, click **Restart**.



- When using SharePoint 2010, the end user will need to disable the **Trusted Documents** setting in order to allow editing of documents on a SharePoint 2010 server using Office 2010,
- When using SharePoint 2007, be aware that the SharePoint 2007 template only allows site navigation, limited editing of the SharePoint site, and upload and download of documents.

Step 2. Create a Web Forward

To create and configure the Web Forward:

1. Log into the [SSL VPN web interface](#).
2. Verify that you have selected the correct user database on the top right of the page.
3. In the **Create Web Forward** section, select the database the users reside in from the **User Database** drop down list.
4. Enter a unique name for the Web Forward in the **Name** field, for example *SharePoint*.
5. Next to **Web Forward Category**: tick the checkbox *Portals* and select *SharePoint 2013* from the list.
6. In the **Hostname** field, enter the hostname or IP address that you wish to connect to.
7. In the **Domain** field, enter the domain that the SharePoint server belongs to.
8. In the **Available Policies** list, choose the policies that you want to apply to the Web Forward and add them to the **Selected Policies** list.
9. Select Yes for **Add to My Favorites** if the Web Forward should be added to the default Resource Category or *No* if this should be configured later.
10. Click **Add**.

The Sharepoint 2013 Web Forward is now visible in the **Web Forwards** section.

How to Configure a Microsoft Exchange OWA Web Forward

The following steps explain the procedure of configuring the Barracuda SSL VPN for use with Microsoft Exchange Outlook Web Access. To configure OWA, you will have to create a Web Forward of type Path-Based Reverse Proxy as explained in the following sections.

In this article:

- [Step 1. Create a Web Forward](#)
- [Step 2. Edit the Web Forward](#)

Related Articles

- [Web Forwards](#)
- [Custom Web Forwards](#)

Step 1. Create a Web Forward

To create and configure the Web Forward:

1. Log into the [SSL VPN web interface](#).
2. Go to the **RESOURCES > Web Forwards** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Create Web Forward** section, select the database the users reside in from the **User Database** drop down list.
5. Enter a unique name for the Web Forward in the **Name** field, for example *Outlook Web Access*.
6. Next to **Web Forward Category**: tick the checkbox *Mail* and select *Outlook Web Access 2010* from the list.
7. In the **Hostname** field, enter the hostname or IP address of the web server you wish to connect to.
8. To save authentication time, select the **Provide Single Sign On** option.
9. In the **Available Policies** list, choose the policies that you want to apply to the Web Forward and add them to the **Selected Policies** list.
10. Select Yes for **Add to My Favorites** if the Web Forward should be added to the default Resource Category or *No* if this should be configured later.
11. Click **Add** to create the Web Forward.

Step 2. Edit the Web Forward

1. In the **Web Forwards** section, click **Edit** next to the Web Forward entry.
2. To use OWA form-based authentication, make sure that the option **Multiple Services On Destination Host** is enabled.
3. Configure additional options, such as authentication parameters if required.
4. Click **Save**.

Adding a resource category to a Web Forward makes it available to the user on the **My Resources** page. You can also configure this Web Forward to be launched automatically every time a user logs into the Barracuda SSL VPN by setting **Auto-Launch** to Yes.

Network Places

Network Places provide remote users with a secure web interface to access the corporate network file shares. With appropriate permissions, users can browse network shares, rename, delete, retrieve and upload files just as if they were connected in the office. In addition, Network Places also provide support for Web Folders and the Windows Explorer Drive Mapping feature. The Barracuda SSL VPN supports the following network file systems:

- SMB (Windows file shares)
- FTP
- SFTP

Web Folders

Web Folders use a direct WebDAV connection. Remote users can access the organization's network through the standard Windows Explorer interface without actually needing to log into the Barracuda SSL VPN. Once configured, they can access the share by clicking an icon and entering their Windows credentials.

Configured Web Folders must go through the Barracuda SSL VPN server so that the share can be seen by the client operating system. For security reasons, the Barracuda SSL VPN only allows Web Folders that are mapped to existing *Network Places*. This enforces policy restrictions; if a user does not have a policy which allows them to access a given network place then they will also be unable to map a Web Folder to it.

Windows Explorer Drive Mapping

The Windows Explorer Drive Mapping feature allows you to create a Network Place and assign it a drive letter for clients running Microsoft Windows. When the Barracuda SSL VPN Agent is running on the client system, the drive becomes available in the Windows Explorer just like any local drive. This feature uses a WebDAV connection to a locally created SSL tunnel that gets routed through to the server.



Windows specifies the maximum file download size of 2 GB. If you need a larger file download size, download and install the [Network Connector](#).

In this Section:

- [How to Create a Network Place Resource](#)
- [How to Configure AV Scanning](#)

How to Create a Network Place Resource

The following steps describe the process of creating and configuring Network Places on the Barracuda SSL VPN in order to allow users access to the companies network shares.



On Windows systems, the Network Places resource provides support for Web Folders and the Windows Explorer Drive Mapping feature. To use these features, the Windows user must have administrative rights.

In this article:

- [Step 1. Create the Network Place](#)
- [Step 2. Edit the Network Place](#)
- [Step 3. Launch the Network Place](#)
- [Step 4. Add the Network Place](#)

Step 1. Create the Network Place

1. Log into the [SSL VPN web interface](#).
2. Go to the **RESOURCES > Network Places** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Create Network Place** section, select the desired database from the **User Database** drop down list.
5. Enter the name of the Network Place in the **Name** field.
6. In the **Path** field, specify the path to the Network Place, for example: `\\sales\\public`.
7. In the **Username** and **Password** fields, enter the username and password, or leave them blank if you want the user to provide credentials when the application is launched. If you are using session variables:
 - a. Select `session:username` in the **Username** field.



You might have to enter the domain as well as the **Username** session variable, using the following format: *domain\{session:username}*

b. In the **Password** field, select *session:password*.

8. In the **Available Policies** section, select the policies that you want to apply to the Network Place and click **Add >>**



If the policy that you want to add is not available in the **Available Policies** section, make sure that the appropriate user database is selected from the pull-down menu in the upper right of the page, or select the *Global View* user database to list all of the available policies from all the user databases.

9. Click **Add** to create the network place.

The Network Place resource is now created and displayed in the **Network Places** section.

Step 2. Edit the Network Place

You can configure additional settings such as host and folder options by completing the following steps:

1. In the **Network Places** section, click the **Edit** link associated with the Network Place. The **Edit Network Places** page opens.
2. Configure the settings as required.
3. When you are finished configuring your options, click **Save** at the bottom of the page.
4. Click **Save**.

Step 3. Launch the Network Place

To test the Network Place, go to the **Network Places** section, click the name of the Network Place or the **Launch** link associated with it. Make sure that you also test a user account that has the appropriate access rights with a connection outside your intranet.

Step 4. Add the Network Place

When you are ready to make the Network Place available to your users, apply a resource to it.

1. In the **Network Places** section, click the **Edit** link associated with the new Network Place.
2. In the **Categories Resource** section, select the resource categories that you want to apply to the Network Place, then click **Add>>**.
3. Click **Save**.

How to Configure AV Scanning

The Barracuda SSL VPN delivers the latest in virus and application definitions through Energize Updates (see [Licensing](#)). When virus scanning is enabled, the Barracuda SSL VPN scans files that are uploaded through the Barracuda SSL VPN for viruses and other malware. You can determine the types of **files to scan** by specifying a pattern or a specific filename. Any file matching one of the current patternS will have the associated action performed on it. To remove a pattern, select it from the corresponding section and click **Remove**.

Configure Virus Scanning

1. Log into the Barracuda SSL VPN Web interface as the *ssladmin* administrative user.
2. Go to the **BASIC > Virus Checking** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Virus Scanning Options** section, select Yes to **Enable Virus Scanning**.
5. Next to **Files to Scan**, enter the patterns or filenames to be scanned for viruses and click **Add >>**.



Specify files by their exact name or combined with the asterisk ("*") as a wildcard that matches any number of any character. For example:

- The file "badfile.html": *badfile.html*
- All files ending in ".exe": **.exe*
- All files starting with "Readme": *Readme**
- Every file: ***

6. If you want files to be excluded, add them to the **Patterns to Exclude** list.

7. In the **Files to Block** section, add the patterns or filenames that should be blocked without any scanning.

Applications

Some tasks require the use of client-server applications. The Barracuda SSL VPN Agent on the client established a secure tunnel to the Barracuda SSL VPN and then launches the application specified by the application resource. Application definitions are regularly updated with [Engrize Updates](#). There are two types of application resources:

Full Application Download

No preinstalled application is necessary. The download automatically starts when the application resource is started. These applications may be limited to just one platform. Some examples for full applications are:

- PuTTY
- UltraVNC
- Firefox Portable

Configuration File Download

For this type of application resource, the application must be preinstalled on the client system. The Barracuda SSL VPN starts the local application on the client and provides a configuration for the resource you want to access. Examples include:

- Microsoft RDP client
- RDP - RDesktop
- Remote Desktop Client v2 for Mac OS X

Next Steps

- [How to Create an Application Resource](#)
- [How to Configure Outlook Anywhere](#)
- [How to Configure ActiveSync for Microsoft Exchange Servers](#)
- [How to Configure Microsoft RDP RemoteApp](#)

How to Create an Application Resource

Application resources are shortcuts to predefined application definitions and the necessary complementary configuration settings. When the user clicks the application resource the application is started with the settings provided by the administrator. Follow these steps to create an application resource.

In this article:

- [Step 1. Create an Application Resource](#)
- [Step 2. \(optional\) Edit Advanced Settings for the Application Resource](#)
- [Step 3. Launch the Application](#)

Step 1. Create an Application Resource

1. Log in to the SSL VPN Web interface.
2. Go to the **RESOURCES > Applications** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Create Application** section, enter a **Name**. E.g., OfficeCitrix
5. Select the application definition from the **Application** list. You may need to click the application category to see the entry in the list. E.g., Citrix Published Applications
6. Enter the required configuration settings. E.g., **hostname** for the Citrix server
7. In the **Available Policies** section, select the policies that you want to apply to the application and click **Add**.
8. Click **Add** to create the application.

The new application resource is created and displayed in the **Applications** section.

Step 2. (optional) Edit Advanced Settings for the Application Resource

In the **Applications** section click the **Edit** link next to the application to configure additional options.

Step 3. Launch the Application

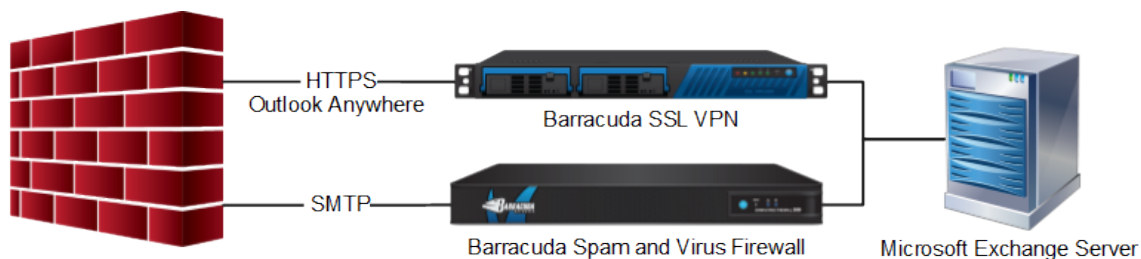
1. In the **Applications** section, click the **Launch** next to the application to test it.
2. When you are ready to make the application available to your users, click the **Edit** link associated with the resource in the **Applications** section.

3. Select the resource categories that you want to apply to the application in the **Resource Categories** section, and then click **Add**.
4. Click **Save**.

How to Configure Outlook Anywhere

To protect the Microsoft Exchange server from the direct external access, you can deploy a [Barracuda Spam and Virus Firewall](#) for all SMTP traffic and a Barracuda SSL VPN to handle all HTTPS traffic coming from the Internet. The client connects to the Barracuda SSL VPN using Outlook Anywhere (formerly known as RPC over HTTPS). Authentication and proxying of all traffic is also handled by the SSL VPN.

Related Articles
• Resources • How to Create an Application Resource



In this article:

- [Before you Begin](#)
- [Step 1. Configure the Barracuda SSL VPN](#)
- [Step 2. Configure the Exchange Server](#)
- [Step 3. Configure the Outlook 2013 Client](#)
- [Step 4. Test the Configuration from an External Network](#)
- [Troubleshooting Outlook Anywhere](#)

Before you Begin

- Make sure that you have a valid SSL certificate signed by a trusted root Certification Authority (CA) or a self-signed certificate. If you are using a self-signed certificate, you must import it to the local certificate store on all the client machines on which you want to use Outlook.
- If required, open port 443 on your internal firewall so that the Barracuda SSL VPN can communicate with the Exchange Server.

Step 1. Configure the Barracuda SSL VPN

Configure the Barracuda SSL VPN to act as an RPC Proxy.

1. Log into the [SSL VPN web interface](#).
2. Open the **Mange System > RESOURCES > Configuration** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Outlook** section:
 - a. In the **Exchange Server** field, enter the Exchange servers hostname.
 - b. In the **Exchange Port** field, enter 443 (unless you have configured the Exchange server to listen on a different port).
 - c. In the **Protocol** area, click the **HTTPS** option.
 - d. In the **Authorized Policies** section, select one or more policies that contain the users that should have access to the Outlook proxy and click **Add** to add them to the **Selected Policies** area.
5. Click **Save Changes**.

Step 2. Configure the Exchange Server

For each Exchange server, complete the following steps:

1. Open the Exchange 2013 web interface.
2. From the left hand panel of the **Exchange admin center** page, go to **servers** and select **servers** from the main menu.

3. Double click the Exchange Server that you want to configure.
4. From the left hand panel of the server configuration window, select **Outlook Anywhere**.
5. Enter the external host name for your Exchange Server, for example: *mail.mycompany.com*.
6. Set the authentication type to *Basic*. By default, authentication is set to *NTLM*, which does not work for clients that are connecting from a different domain than the Exchange Server.

Step 3. Configure the Outlook 2013 Client

On the client's Windows system, configure the Outlook 2013 client:

1. Open the **Control Panel**
2. Double-click the **Mail**.
3. Click **Show Profiles**
4. Click **Add** to add a new mail profile.
5. Enter a unique **name** for the mail profile and click **OK**.
6. Select the **Manually configure server settings or additional server types** option and click **Next**.
7. Select the **Microsoft Exchange or compatible service** option and click **Next**.
8. In the **Server** field, enter the Barracuda SSL VPN hostname, for example: *sslvpn.example.com*
9. In the **User Name** field, enter your username in the following format: *username@domain*. Do NOT click **Check Name**.
10. Click **More Settings**
11. Select the **Connection** tab.
12. In the **Outlook Anywhere** section, select the **Connect to Microsoft Exchange using HTTP** option and click **Exchange Proxy Settings**.
..
13. In the **Connection settings** section, complete the following steps:
 - a. In the **Use this URL to connect to my proxy server for Exchange** field, enter the Barracuda SSL VPN hostname.
 - b. Check the option for **On fast networks, connect using HTTP first, then connect using TCP/IP**.
 - c. Check the option for **On slow networks, connect using HTTP first, then connect using TCP/IP**.
 - d. In the **Proxy authentication settings** area, select *Basic Authentication* from the **Use this authentication when connecting to my proxy server for Exchange** drop-down menu.
 - e. Click **OK** and then click **Next**.
14. The **Exchange Server** prompts you to connect and requests your credentials:
 - a. In the **User Name** field, enter your username using the following format: *domain\username*
 - b. In the **Password** field, enter your password and click **OK**.
15. Click **Finish** and then click **OK**.

Step 4. Test the Configuration from an External Network

Use the following procedure to determine if your Outlook 2013 clients are successfully connecting to your Exchange Server 2013 using Outlook Anywhere:

1. From the command line, start **outlook.exe /rpcdiag**. The Outlook email client and an extra diagnostic window opens. Keep this window open to test your configuration.
2. If prompted, select the new Outlook profile and click **OK**.
3. The Exchange Server prompts you to connect and requests your credentials. Using the format *domain\username*, type your username and password, and click **OK**. The Outlook client then retrieves the client's email from the Exchange Server through the Outlook Anywhere connection.
4. Check the **Connection Status** window.

When the Outlook client is fully connected, you will see 4 connections (2 Mail types and 2 Directory types) to your Exchange Server. All of these connections should show a connection (**Conn**) type of HTTPS. If they do, the test is successful.

Troubleshooting Outlook Anywhere

If the connection type is TCP/IP, then the Outlook client is connected directly to the Exchange Server and is not using RPC. If this is the case, verify the following points to troubleshoot the issue:

- Verify your Outlook 2013 client configuration.
- Verify your Exchange Server 2013 configuration.
- Verify that you have a valid SSL certificate signed by a trusted root Certification Authority (CA) or a self-signed certificate installed on the Barracuda SSL VPN.
- If you are using a self-signed certificate, verify that you have imported it to the local certificate store on

all the client systems that are using Outlook 2013.

- If required, verify that you have opened port 443 on your internal firewall for the Barracuda SSL VPN to communicate with your Exchange Server.
- Make the appropriate Outlook and Exchange Server configuration changes, and test your configuration from your external network.

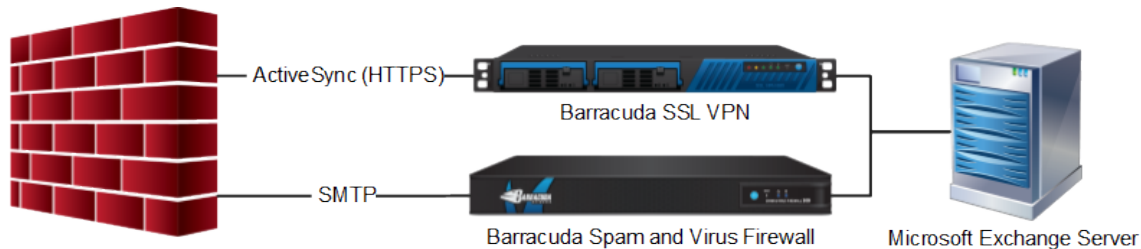
How to Configure ActiveSync for Microsoft Exchange Servers

If you are using Microsoft Exchange Server, your users can securely access their email, calendar, contacts and tasks from their mobile devices using Microsoft Exchange ActiveSync via the Barracuda SSL VPN. ActiveSync allows mobile users to securely connect to an Exchange server. As an added layer of security, you can use the Barracuda SSL VPN to authenticate ActiveSync requests and proxy all the traffic. The advantage of this deployment is that only the Barracuda SSL VPN will accept HTTPS traffic from the Internet.

Related Articles

- [Resources](#)
- [How to Create an Application Resource](#)

When used in combination with a Barracuda Spam and Virus Firewall protecting the Exchange servers from direct external access.



In this article:

- [Before you Begin](#)
- [Step 1. Configure the Barracuda SSL VPN](#)
- [Step 2. Configure Exchange Server 2013](#)
- [Step 3. Configure the Client Mobile Device for ActiveSync](#)
 - [Connecting an Android Mobile Device](#)
 - [Connecting an Apple iOS Device](#)
- [Special Case: Multiple User Databases](#)

Before you Begin

- Make sure that you have a valid SSL certificate signed by a trusted root Certification Authority (CA) or a self-signed certificate. If you are using a self-signed certificate, you must import it to the local certificate store on all the client machines on which you want to use Outlook.
- If required, open port 443 on your internal firewall so that the Barracuda SSL VPN can communicate with the Exchange Server.

Step 1. Configure the Barracuda SSL VPN

Configure the Barracuda SSL VPN to allow Outlook Anywhere access (see **Step 1.** of [How to Configure Outlook Anywhere](#)).

Step 2. Configure Exchange Server 2013

For each Exchange server, configure the settings as described in **Step 2.** of [How to Configure Outlook Anywhere](#).

Step 3. Configure the Client Mobile Device for ActiveSync

Follow the instructions below for the type of mobile device that you want to connect to the Barracuda SSL VPN.

Connecting an Android Mobile Device

To set up your Exchange ActiveSync account on your Android device, proceed as follows:

1. On your Android device, start **Settings** and scroll to the **Accounts** section.
2. Tap **Add Account**, then **Corporate**. Type in your email address and password and click **Next**.
The mobile device attempts to retrieve the account information and does not succeed.
The device prompts for further information.
3. Type in your Active Directory domain name in front of your username so that it is in the format: domain\username
4. For **Server**, type in the SSL VPN hostname. e.g., sslvpn.example.com
5. Verify **Use secure connection (SSL)** is selected. If you are using a self-signed certificate, select **Accept all SSL certificates**.
6. Tap **Next**.
The device will now prompt "The server <sslvpn hostname> requires that you allow it to remotely control some security features of your Android device. Do you want to finish setting up this account?"
7. Tap **OK**.
8. Configure the Account Options and tap **Next**.
9. Tap **Next**.

You can now access your email using the Android Mail Application.

Connecting an Apple iOS Device

Follow these steps to set up your Exchange ActiveSync account on your Apple iPhone, iOS device or iPod Touch:

1. On your iOS device, tap **Settings > Mail, Contacts, Calendars > Add Account... > Microsoft Exchange**.
2. In the window that appears, enter your **Email**, **Username** and **Password**, where **Email** and **Username** are your full email address (for example: somebody@example.com). Tap **Next**.
The iOS device tries to verify the account, fails and prompts you to enter some extra details.
3. Complete the following fields and then tap **Next**.
 - **Server** - Type in your company's Barracuda SSL VPN hostname (for example: mysslvpn.example.com).
 - **Domain** - Type in the Active Directory domain name (for example: example.com).
4. This time the settings are verified. Select which items to synchronize between your account and your device and tap **Save**.

You can now access your email by opening the Mail Application.

Special Case: Multiple User Databases

Many customers only use one user database. However, If you are using multiple user databases, then you need a different hostname for each user database that you want to use with ActiveSync, except for the default user database.

As an example, if your Barracuda SSL VPN uses the hostname sslvpn.example.com, then you may choose something like ad1.sslvpn.example.com as a user database hostname. You will also need to create a publicly-available DNS entry that maps ad1.sslvpn.example.com to the IP address of the Barracuda SSL VPN.

You can tell if a user database is set as default by looking at **ACCESS CONTROL > User Databases**. The user databases that are not built-in have a **More..** menu to the right hand side. If you click on that, and it displays an option to set this user database as default, then this is not the default database.

1. Navigate to **ACCESS CONTROL > User Databases**. The **User Databases** section shows the built-in databases and the user databases that you have already configured. If there is an **Edit** option on the same row as the relevant user database, click it.
2. In the **User Database Details** section, enter a hostname in the **User Database Host** field. This is normally a subdomain of your Barracuda SSL VPN hostname.
3. Add an entry for this hostname in your external DNS servers so that it resolves to the public IP address of the Barracuda SSL VPN.
4. When connecting mobile devices to the Barracuda SSL VPN, use this new user database hostname as the server address.

How to Configure Microsoft RDP RemoteApp

Microsoft Windows Server 2008 R2 added a feature that allows organizations to deploy server hosted desktop applications without requiring the user to load an entire remote desktop. Only the application window is remotely displayed, integrating seamlessly into the user's current desktop. This feature is only available when using the Microsoft RDP client.

Before you Begin

Create a rdp file on the Microsoft Windows Server for the application you want to use via RDP RemoteApp.

Create a new Application Resource

Create a standard RDP application resource using the Microsoft RDP Client Application template.

1. Open the **RESOURCES > Applications** page.
2. Enter a **Name**. E.g., RDP RemoteApp
3. Select **RDP - Microsoft RDP Client** from the **Application** list.
4. Enter the **Hostname**.
5. Select the policies this resource should be available for and click **Add**. The policies are now visible in the **Selected Policies** list.
6. Click **Add**.

Add the RemoteApp Configuration to the Application Resource

Use a text editor to open the rdp file and then complete the following steps to configure the RemoteApp on the Barracuda SSL VPN:

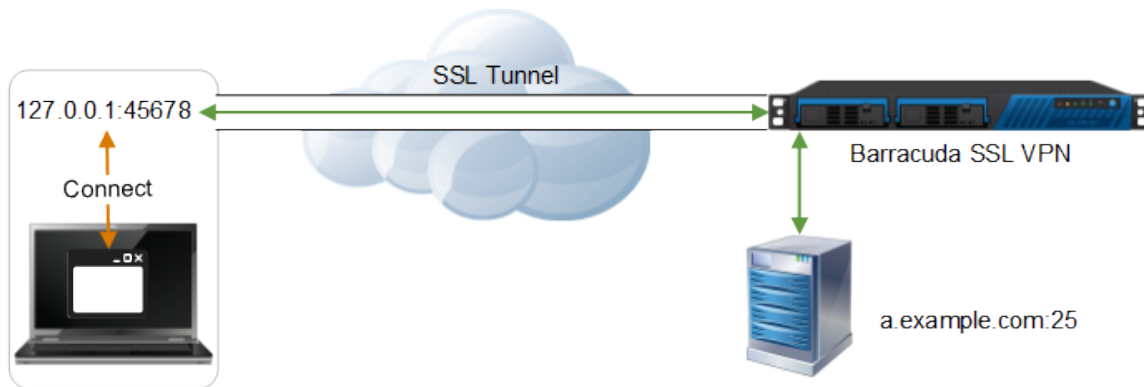
1. In the **Applications** section click **Edit** for the RDP application resource you just created. E.g., **RDP RemoteApp**
2. In the **Remote Applications** section enter:
 - **Remote Applications Mode** – Select **Yes**.
 - **Remote Application Name** – Enter the *remoteapplicationname* value after the last colon from the rdp file created on the Windows Server. E.g., Navision if the string in the rdp file is: remoteappliationname:s:Navision
 - **Remote Application Program** – Enter the value after the last colon of *remoteapplicationprogram* in the rdp file created on the Windows Server. E.g., Navision PDP Systems USA if the string in the rdp file is: remoteapplicationprogram:s:|Navision PDP Systems USA.
 - **(optional) Command Line Arguments** – Enter optional commandline arguments which will be passed to the applications when it is started.
3. Click **Save Changes**.

All users included in the policies attached to this application resource can now run the RemoteApp on the Windows Server via the Barracuda SSL VPN.

SSL Tunnels

SSL Tunnels are used to encrypt data for client/server applications which normally do not use encryption. The tunnel is created by the SSL VPN Agent and terminated at the Barracuda SSL VPN (local tunnel). The remote user does not connect directly to the remote resource as in a VPN,

but to a Port on the 127.0.0.1 interface. The SSL VPN Agent accepts the local connection and forwards the traffic through the SSL tunnel. The Barracuda SSL VPN forwards the traffic to the destination IP and Port defined in the SSL tunnel configuration. The traffic from the Barracuda SSL VPN to the destination IP in the network is not encrypted anymore.



SSL tunnels can be configured to only allow local connections or to allow connections directly to the remote network. It is also possible to define the source IP address of the SSL tunnel, so that clients in the same remote network can share a SSL tunnel. The tunnel is terminated when the session is closed or timed out.

Next Steps

To create a SSL Tunnel complete the following instructions: [How to Create an SSL Tunnel](#).

How to Create an SSL Tunnel

An outgoing SSL tunnel protects TCP connections that your local computer forwards from a local port to a preconfigured destination IP address and port, reachable by the Barracuda SSL VPN that the user is connected to. To use the tunnel, the application or browser connects to a random listener port on the 127.0.0.1 or 127.0.0.2 localhost address. The encrypted tunnel ends at the SSL VPN, all connection beyond the SSL VPN are not secure. If you want other computers on the same network to share a SSL tunnel, use a network IP address instead of the 127.0.0.1 localhost address as the source address.

In this article

- [Step 1. Create a SSL Tunnel](#)
- [Step 2. \(Optional\) Configure Advanced Tunnel Settings](#)
- [Step 3. Test the SSL Tunnel](#)

Step 1. Create a SSL Tunnel

1. Log into the [SSL VPN web interface](#).
2. Go to the **RESOURCES > SSL Tunnels** page.
3. In the **Create SSL Tunnel** section, select the desired database from the **User Database** drop down list.



If you are a Super User in the Global View and you want to apply this SSL tunnel across more than one User Database, select *Global View* as the User Database to list the Policies across all the User Databases.

4. Enter a unique name for the tunnel in the **Name** field.
5. In the **Destination Host** field, enter the name or IP of the resource you want to access.



The `$$` indicates that replacement variables can be used. Clicking this icon will load the replacement variables that are available. The *session* variables are values taken from the current session. The *userAttributes* variables are values taken from user-defined attributes for the currently logged on user.

6. In the **Destination Port** field, enter the port number on the destination host. If you have a client application running on the destination host that for example listens at port 5900 for VNC, enter 5900.
7. Select Yes for **Add to My Favorites** if the tunnel should be added to the default **Resource Category**.
8. Double-click on your desired policies from the **Available Policies** list to send them to **Selected Policies** list.
9. Click **Add** to create the SSL Tunnel.

The SSL tunnel is now visible in the **SSL Tunnel** section.

Step 2. (Optional) Configure Advanced Tunnel Settings

You can configure additional settings such as **auto launch**, **multiple port ranges** or **tunnel type** by editing the SSL tunnel configuration:

1. In the **SSL Tunnels** section, click the **Edit** link associated with the tunnel. The **Edit Tunnel** page opens.
2. Configure the settings as required.
3. Click **Save**.

Step 3. Test the SSL Tunnel

To test the SSL tunnel, click the name of the SSL Tunnel you just created or the **Launch** link associated with it. Make sure that you also test a user account that has the appropriate access rights with a connection outside your intranet.

Remote Assistance



Remote Assistance only works on Windows and Linux-based computers with Oracle Java installed. Mac OS X users cannot successfully initiate a remote assistance session.

Remote Assistance (RA) is a standard help desk feature on the Barracuda SSL VPN. It enables remotely-connected users to easily communicate with their IT department. System administrators and help desk personnel can see at a glance which users are in need of help, communicate with a remote user via instant messages and, if needed, view and control the remote system directly to resolve various issues.

Requirements for Remote Assistance

- The Barracuda SSL VPN Agent requires the Oracle Java Virtual Machine (JVM) to be installed on both the remote and the help desk systems in order for the two-way communication tunnel to be initiated. Specialized VNC client/server software is used to access and control the remote system. The VNC clients and server is downloaded as needed from the Barracuda SSL VPN requiring no separate installation.
- Because the VNC application is downloaded on demand, the user of the remote system must have administrator/root rights.
- The user must have the appropriate Access Rights to provide or request Remote Assistance. Additionally, it is recommended that you configure policies for users and Helpdesk administrators and assign them either the Access Right *Remote Assistance Administration* or *Request Remote Assistance* when editing a policy. For more information, see [How to Configure Policies](#).

In this Section:

- [Requesting Remote Assistance](#)
- [Providing Remote Assistance](#)

Requesting Remote Assistance

Any user account that is granted the Access Right *Remote Assistance Create*, will have the ability to access their own **My Remote Assistance** page where they can create, modify and submit their own remote assistance requests. (For information on how to configure Access Rights, see [Access Rights](#).)

To create a remote assistance request, complete the following steps:

- [Step 1. Create a Remote Assistance Request](#)
- [Step 2. Launch the Remote Assistance Request](#)

Related Articles

- [Remote Assistance](#)
- [Providing Remote Assistance](#)

Step 1. Create a Remote Assistance Request

1. Log into the [SSL VPN web interface](#).
2. Open the **RESOURCES > My Remote Assistance** page.
3. In the **Name** field, enter a brief summary for your request.
4. Add a detailed description of the problem and any additional notes concerning this request.
5. Enter your **email** address and **phone** number (optional).
6. Click **Add**.

The request is added to the **My Remote Assistance Requests** section.

Step 2. Launch the Remote Assistance Request

As soon as the helpdesk administrator has contacted you and requests access to your system,

1. Click on your remote assistance request to launch the session.
2. Once the assistance session has started, you can communicate with the assistant. Click the **Chat** icon on the bottom of the screen to view and send messages.

When the session is closed, the request will be deleted from the list.

Providing Remote Assistance

A helpdesk- or system administrator with the appropriate access rights can respond to remote assistance requests sent by standard users and then connect to the remote system to provide assistance. All modifications to a request will trigger an email notification to both the owner of the request as well as to the assigned assistant. In order to provide remote assistance, the assistant must have the following **Resource Rights** (see [Access Rights](#)):

Related Articles
• Remote Assistance • Requesting Remote Assistance

- *Remote Assistance Create* - Allows creating of assistance requests for other users.
- *Remote Assistance Edit* - Allows editing of the details of an assistance request that has been submitted, such as the assigned assistant, the scheduled time and the status of the request.
- *Remote Assistance View* - Allows viewing of all existing assistance requests, as well as connecting to a remote system that is requesting assistance.
- *Remote Assistance Delete* - Allows closing of any assistance requests that are still open.

To provide remote assistance, complete the instructions given in the following steps:

- [Step 1. Access the Remote Assistance Request](#)
- [Step 2. Connect to the Remote System](#)
- [Step 3. Close the Remote Assistance Request](#)
- [Create a Request for other Users](#)

Step 1. Access the Remote Assistance Request

1. Log into the [SSL VPN web interface](#).
2. Go to the **RESOURCES > Remote Assistance** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. Check the **Remote Assistance Requests** section. The list displays all requests that have been submitted by standard users and allows editing of the details, such as the assigned assistant, status and scheduled time. The **Available From** column displays the requested times of assistance. An asterisk (*) means that no specific time is requested.
5. To view and modify the details click the **Edit** link next to the request.

Step 2. Connect to the Remote System

To work on an assistance request, you will generally require a direct connection to the remote system.

1. To initiate the connection, click the **Launch** link associated with the request. This will set the status to *Waiting for Connection*. When the user responds, the status will be set to *In Progress*, and an RDP session to the remote system still be launched. You may refresh the page to see the status change.
2. Once the assistance session has started, select *Show Chat Window* from the taskbar from the **View** context menu under **Remote Assistance**. You can now communicate with the user.
3. To send files via the chat client in the **Remote Assistance** window, select *Send File* from the **Connection** context menu.

Step 3. Close the Remote Assistance Request

When the assistance session has finished, terminate the connection by closing the **Remote Assistance** window. (This will also set the status to *Inactive* if the **One-Time Request** field is set to *No*.) Once the request is closed, it will be deleted from the list.

Create a Request for other Users

As a helpdesk administrator, you can also create remote assistance requests for other users if required:

1. Enter a brief summary of the nature of the request in the **Name** field.
2. Enter the name of the account for which this request is being created in the **Username** field.
3. In the **Email** field, enter the user's email address. Any notifications regarding this request will be sent to the address entered here.
4. If this request can be handled at any time, set **Start Immediately** to Yes, otherwise, set to *No* to activate the **Preferred Time** field and specify the appropriate values. (Set to blank to request assistance to begin as soon as possible.)
5. Click **Add**.

Network Connector

The Network Connector provides full, transparent access for users requiring general or more widespread network access. No configuration is required on the client computer, the configuration is stored on the Barracuda SSL VPN. Authorized users can be provided with complete TCP/UDP access to the entire network in a manner similar to what is provided by IPsec, including mounting drives, accessing network shares and moving files, just as if they were physically inside the companies network.

Deployment

The Network Connector consists of two components:

- A *server-side* component which needs to be enabled on the Barracuda SSL VPN to allow access by your designated users.
- A *client-side* component that, when installed onto the remote system, connects to the server interfaces.

When a client connects to the Barracuda SSL VPN with the Network Connector, it is assigned a secondary IP address from the IP range defined in the network connector resource configuration. The network connector uses the assigned secondary IP and the configured published routes to determine which traffic to forward to the internal network. The default configuration is for the network connector to act as a split level VPN, only routing traffic destined for the internal network through the tunnel. It is possible to change this behavior to route all traffic through the network connector.

In this Section

- [How to Configure the Network Connector](#)
- [How to Create a Static Route](#)
- [Advanced Network Connector Client Configuration](#)
- [Using the Network Connector with Microsoft Windows](#)
- [Using the Network Connector with Mac OS X](#)
- [Using the Network Connector with Linux](#)

How to Configure the Network Connector

Configure the server side settings for the network connector and create the client configurations. Supported platforms are Windows, Linux and Mac OS X.



The displayed **Network** and **IP Address** are those already assigned to the Barracuda SSL VPN. The IP addresses distributed by the Network Connector to remote systems must be a subnet of the IP address range that you assigned to the unit in the administrative interface. For example:

Barracuda SSL VPN IP configuration: 10.0.0.1 with netmask 255.255.255.0

Available: IPs for the Network Connector LANs: 10.0.0.2 - 10.0.0.254

Related Articles

- [How to Create a Static Route](#)
- [Advanced Network Connector Client Configuration](#)
- [Using the Network Connector with Microsoft Windows](#)
- [Using the Network Connector with Linux](#)
- [Using the Network Connector with Mac OS X](#)

Configuring a New Network

1. Log into the [SSL VPN web interface](#).
2. Navigate to the **RESOURCES > Network Connector** page.
3. Click **Configure Network** to bring up the **Create Network Configuration** page.
4. In the **Server Information** section, configure the network information that will apply to your remote users:
 - a. In the **IP Address Range Start** and **End** fields, enter the first and last IP addresses of a DHCP range that can be assigned to remote systems. All Network Connector IP addresses will be assigned from a DHCP range that is derived from this information. To prevent IP conflicts, the specified range must NOT be a part of any other existing DHCP range.
 - b. If you want your remote users to default to using a different domain name and DNS server, enter your desired values for **Domain Name** and **Primary DNS Server**.



The default values are derived from the values already assigned to the Barracuda SSL VPN. The domain name configured here will be used whenever a requested system is identified only by its system name without the domain portion (i.e., not as an FQDN), and the primary DNS server will be used to resolve all supplied hostnames.

5. From the **Available Policies** area, select the policies that contain the users who should be allowed access to this Network Connector configuration and click **Add >>** to add them to the **Selected Policies**.
6. Click **Save** when you are done.

This will create a LAN entry in the **Server Interfaces** section, and a corresponding LAN client entry in the **Client Configurations** section. As soon as a server interface is created, you can customize the configuration according to your requirements:

- You can create (or copy) and configure your client settings as required. For more information, see [Advanced Network Connector Client Configuration](#).

How to Create a Static Route

If the Barracuda SSL VPN is installed in a DMZ, you must create a static route on the client systems so that they can reach the main LAN. To introduce the static route, complete the following steps:

- [Step 1. Configure the Client](#)
- [Step 2. Configure the Static Route](#)
 - [Option 1: Publish the Static Route](#)
 - [Option 2: Configure an Up Command for the Static Route](#)

Related Articles

- [Network Connector](#)
- [How to Configure the Network Connector](#)

Step 1. Configure the Client

Configure the client as described in [Advanced Network Connector Client Configuration](#). At this point the client will only be able to route through to other systems within the DMZ. Before creating a static route on the client systems, determine the default gateway address that the Barracuda SSL VPN uses. This gateway should be able to route to the main LAN from the DMZ. To create a route to the clients to tell them how to get to the main LAN, there are two alternatives:

- Publish a route that will apply to all clients using this Network Connector server interface.
- Use an *Up Command* in the client configuration that configures the route on the client when the network connector is launched.

Step 2. Configure the Static Route

Option 1: Publish the Static Route

To publish a static route for all users of a server interface:

1. Go to the **RESOURCES > Network Connector** page.
2. Click **Edit** next to the relevant server interface.
3. On the **Edit Server Interface** page, in the **Routing Section**, specify the network to be published. This network will always use the default gateway. All clients will use this route, so if you have multiple client configurations with different networks, you may need to use the *Up Command* instead.

Option 2: Configure an Up Command for the Static Route

To configure an *Up Command* to create a static route on the client system when the configuration file is launched, proceed as follows:

1. From the Barracuda SSL VPN web interface, log in as *ssladmin* and verify that you are in the **Manage System** mode.
2. Go to the **RESOURCES > Network Connector** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Edit Client Configuration** section, add the *Up Command*.

Example:

- DMZ network address of *192.168.1.0/24*
- Barracuda SSL VPN on IP address *192.168.1.100* and default gateway of *192.168.1.1*
- Main LAN network address of *192.168.50.0/24*

The *Up Command* to publish for such a route would be:

- For Windows clients:
route add *192.168.50.0* mask *255.255.255.0* *192.168.1.1*
- For Linux/Mac clients:
route add -net *192.168.50.0* netmask *255.255.255.0* gw *192.168.1.1*

5. **Save** the configuration.

When launched, this configuration should automatically publish this new route 10-15 seconds after the Network Connector client is launched.

Advanced Network Connector Client Configuration

A default client configuration is automatically generated when the network connector is created; however, you may need to edit this configuration to make it suitable for the majority of your users. Additional client configurations may also be required in some instances, such as for remote users on different platforms that may require different initialization commands. You can create additional additional client configurations for the same Server Interface by copying (click the **Copy** link associated with the client) the initial client configuration, and then customizing it.

In this article:

- [Client Settings](#)
- [Up- and Down Commands](#)

Related Articles

- [Network Connector](#)
- [How to Configure the Network Connector](#)
- [How to Create a Static Route](#)

Client Settings

The following additional client settings can be configured by editing the network connector client configuration.

Setting	Description
---------	-------------

Auto-Launch	This setting determines whether a user logging in to the Barracuda SSL VPN will automatically launch the Network Connector. This does not affect the ability of the stand-alone version of the Network Connector from also running with this particular client configuration.
Server Interface	The server interface identifies the network information that this client configuration is associated with. This should match the server interface that caused the creation of this client configuration.
Static IP Address	This field should only be used when you expect only one remote user to connect using this configuration. If there is a value specified here, then the remote system that is connecting via the Network Connector will always be assigned this IP address, regardless of any DHCP range that is set in the associated server interface.
Authentication Type	If you wish to change the authentication type for the user of this client configuration, then select the desired method here.

Up- and Down Commands

Up commands are executed from a temporary script file created by the Barracuda SSL VPN when a remote client connects with the Network Connector. This script can be used to create the needed static routes when the Barracuda SSL VPN is installed in a DMZ. For more information, see [How to Create a Static Route](#).

Down commands are executed when the remote client disconnects, usually to remove settings added by the up commands.

Command	Description
Up	In the Up Commands area, you can enter any command that is executable from a script file. These can range from initializing environment variables, to adding network printers and mapping of network drives. Example 1: Up command to publish a route: - Windows clients: <code>route add 192.168.50.0 mask 255.255.255.0 192.168.1.1</code> - Linux/Mac clients: <code>route add -net 192.168.50.0 netmask 255.255.255.0 gw 192.168.1.1</code> Example 2: Up command for Mac clients (xx.xx.xx.xx and example.com are the DNS server IP and DNS suffix): <pre>#!/bin/bash -x mkdir -p /etc/resolver echo "nameserver xx.xx.xx.xx" > /etc/resolver/example.com killall lookupd exit 0</pre>

Down

In the **Down Commands** area, enter the commands that you want the remote system to execute when leaving the secured network. Typically, you will have a corresponding Down command for every Up command that was configured, to reverse any action that was taken.

Example 1: Down command to delete a route:

- Windows clients: `route delete 192.168.50.0 mask 255.255.255.0`
- Linux/Mac clients: `route del -net 192.168.50.0 netmask 255.255.255.0 gw 192.168.1.1`

Example 2: Down command for Mac clients (example.com is the DNS suffix):

```
#!/bin/bash -x
rm -Rf /etc/resolver/example.com
killall lookupd
exit 0
```

Using the Network Connector with Microsoft Windows



Installing and running the Network Connector service on a Windows system requires the use of an account with administrative permissions.

You can launch the client portion of the Network Connector remotely in one of two ways:

- By signing into the Web interface of the Barracuda SSL VPN and launching the Network Connector.
- By running the Network Connector in stand-alone mode.

For both launch options, you must have the Windows client installed on your remote system.

In this article:

- [Step 1. Install the Windows Client](#)
- [Step 2. \(optional\) Install the Client Configuration File](#)
- [Step 3. Launch the Network Connector Client](#)

Related Articles

- [Network Connector](#)
- [Using the Network Connector with Linux](#)
- [Using the Network Connector with Mac OS X](#)

Step 1. Install the Windows Client

If you are the administrator you can download the Windows client software from the SSL VPN web interface:

1. Log into the [SSL VPN web interface](#).
2. Open the **RESOURCES > My Network Connector** page.
3. Click **Download Windows Client**. You will be prompted to either *Run* or *Save* the installer.
4. Launch the installer once the installation package downloads, and select all default settings as you continue through the installation. If you see warnings about any compatibility issues during the install, click **Continue Anyway**.

Once installed, the Network Connector is ready for use on the remote system as long as you are logged in through the web interface of the

Barracuda SSL VPN.

Step 2. (optional) Install the Client Configuration File

To run the Network Connector in stand-alone mode, without having to log in through the web interface, you must download and install a client configuration file onto the remote system.

 This file is only required for stand-alone mode.

To install the client configuration file on your system:

1. Log in to SSL VPN web interface.
2. Go to the **RESOURCES > My Network Connector** page.
3. Locate the client configuration in the **My Network Connector** section and click **More**.

 When installing the configuration file, you may be presented with various warnings depending on the security level that is configured on your system. Accept the warnings as they appear in order to continue with the installation.

4. Select **Install Client Configuration file**.

Step 3. Launch the Network Connector Client

Once the Client Configuration file is installed, launch the Network Connector client in stand-alone mode:

1. Start the **Network Connector GUI** program. A red network icon will appear in your System Tray.
2. Right-click on that icon and select **Connect**.
3. Enter your authentication information, and click **OK**.
4. The icon will flash while attempting to establish a connection, and will turn green when a secure connection to the protected network is in place and ready for use.

 Due to restrictions imposed by Windows networking, the VPN routes are not instantly published when the Network Connector is launched. Expect to wait around 10-15 seconds after launching the client before the routes are published and the Network Connector client is fully usable.

Using the Network Connector with Mac OS X

Follow these instructions to install the network connector on your Mac:

In this article:

- [Step 1. Install the Mac Client](#)
- [Step 2. Install the Client Configuration File](#)
- [Step 3. Launch the Network Connector Client](#)

Step 1. Install the Mac Client

1. Open the **RESOURCES > My Network Connector** page.
2. Click the **Download Mac Client** button. You will be prompted to either *Run* or *Save the installer (.dmg file)*.
3. Launch the installer once the installation package downloads, and select all default settings as you continue through the installation.

Once installed, the Network Connector is ready for use by any user on the remote system who is logged in through the web interface of the Barracuda SSL VPN.

Related Articles

- [Network Connector](#)
- [Using the Network Connector with Linux](#)
- [Using the Network Connector with Microsoft Windows](#)

Step 2. Install the Client Configuration File



A client configuration file for the Network Connector is required only when using the Network Connector in stand-alone mode.

To be able to run this client in stand-alone mode, or without requiring an explicit login through the web interface, you must install a configuration file for the client on the remote system.

1. Log back into the [SSL VPN web interface](#).
2. Go to the **RESOURCES > My Network Connector** page.
3. Hover over the icon for the client configuration file in the **My Network Connector** section. A list of actions will appear.
4. Select **Install Client Configuration file**. When installing the configuration file, you may be presented with various warnings depending on the security level that is configured on your system. Accept the warnings as they appear in order to continue with the installation.

Step 3. Launch the Network Connector Client

1. Select **Finder > Applications > Network Connector**. A gray network icon will appear in the top right of your screen.
2. Click the network icon and choose **Connect LAN1 Client** (where *LAN1* may be a different network name, depending on how it was configured by *ssladmin*).
3. Enter your username and password when prompted, and click **OK**.

Using the Network Connector with Linux



The Network Connector is available for use with Linux 2.4 or higher integrated with the TUN/TAP driver.

No separate client software is needed to connect from Linux systems to the Network Connector service, since most modern Linux distros already contain the required support in the OpenVPN NetworkManager-openvpn packages. However, a configuration file must be installed in order for the system to connect to the Barracuda SSL VPN.

In this article:

- [Step 1. Install OpenVPN NetworkManager](#)
- [Step 2. Download Client Configuration File](#)
- [Step 3. Configure Network Manager](#)
- [Step 4. Initiate the Connection](#)

Related Articles

- [Network Connector](#)
- [Using the Network Connector with Mac OS X](#)
- [Using the Network Connector with Microsoft Windows](#)

Step 1. Install OpenVPN NetworkManager

If it is not already installed on your system, install OpenVPN NetworkManager. Depending on your Linux distribution, you may need to do this via one of the following methods:

- **Deb based Linux distributions (Ubuntu, Debian,...)** – In a terminal enter: `sudo apt-get install network-manager-openvpn`
- **RPM based Linux distributions (Redhat, SUSE,...)** – In a terminal enter (as root): `yum install NetworkManager-openvpn`

Step 2. Download Client Configuration File

Download and save the client configuration file for the network connector:

1. Log into the [SSL VPN web interface](#).
2. Go to the **RESOURCES > My Network Connector** page.
3. In the **My Network Connector** section, click on the **More...** link next to the client configuration file.
4. Select **Download Client Configuration file** from the list.
5. Save and extract the downloaded file to the users home directory. E.g., `$HOME/SSLVPN`.

Step 3. Configure Network Manager

Configure the Network Manager applet on your Linux system. Exact steps may vary based on your particular Linux distribution, but the resulting settings should be equivalent.

1. Left-click on the *Network Manager* entry on your Linux system panel and select **VPN Connections > Configure VPN**.
2. Click **Import**.
3. Select the Linux ovpn configuration file. E.g., `$HOME/SSLVPN/linux-<Network Connector name>.ovpn`
4. Enter the **Username** and **Password**.
5. Click **Save**.

Step 4. Initiate the Connection

Initiate a secured connection through the Barracuda SSL VPN:

1. Left-click on the *Network Manager* entry on your Linux system panel and select **VPN Connections > Name-for-your-VPN-Connection**.
2. An animated icon will appear while the connection is being made.
3. When connected, the icon will change to show a padlock.

How to Configure IPsec

You can configure the Barracuda SSL VPN to allow L2TP/IPsec connections from remote devices using an L2TP/IPsec client that supports using a pre-shared key (PSK) as an authentication protocol. L2TP/IPsec clients are also standard on most smartphones, including Apple iPhones and iPads, smartphones running Android 1.6 or higher and tablets running Android 3.0 or higher.

In this article:

- [Before you Begin](#)
- [Step 1. Configure the IPsec Server](#)
- [Step 2. Create an L2TP/IPsec Connection](#)
- [Step 3. Apply the Installation to the Client Device](#)

Before you Begin

On your organization's firewall, allow authentication traffic to and from the Barracuda SSL VPN. UDP over ports 500 and 4500 must be enabled to reach the Barracuda SSL VPN for L2TP/IPsec connections to function.

Step 1. Configure the IPsec Server

On the Barracuda SSL VPN, configure the IPsec server to allow your remote users to authenticate and connect to the protected network:

1. Log into the [SSL VPN Web interface](#).
2. Navigate to the **RESOURCES > IPsec Server** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Create IPsec Server** section, enter a descriptive name for your IPsec server.
5. Enter the preshared key. The string must be alphanumeric.
6. In the **IP Range Start/End** fields, enter the first and last IP address of the DHCP range that should be assigned to remote systems connecting via IPsec.

i This IP range must reside in the network range that is configured in the **TCP/IP Configuration** of the appliance interface, and **MUST NOT** be part of any other DHCP range on your LAN.

7. From the **Policies** list, select the available policies that you want to apply to the IPsec server, and add them to the **Selected Policies** list.
8. Click **Add**.

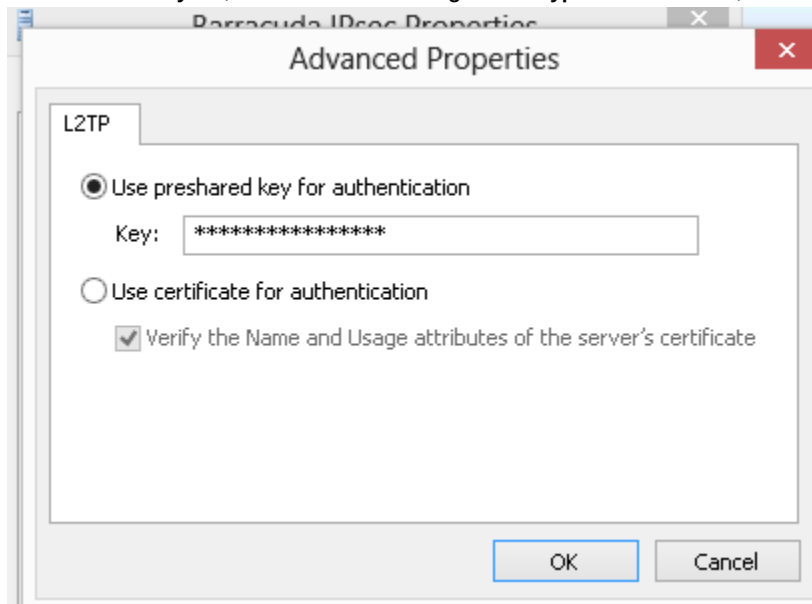
The IPsec Server is now created and appears in the **IPsec Server** section. You can test the configuration by clicking the **Launch** link associated with the entry.

Step 2. Create an L2TP/IPsec Connection

On your remote device, create an L2TP/IPsec connection to the Barracuda SSL VPN.

i If the remote device has had a VPN client *uninstalled* at some point, then make sure that the IPsec service has been re-enabled in order to allow connections via L2TP/IPsec.

1. Log into the Barracuda SSL VPN on the client device.
2. Go to the **Resources** tab.
3. From **My Resources**, select the IPsec server and click to launch it.
During the connection, you will be prompted with a certificate warning message:
 - a. Go to your network connections, right click the SSL VPN connection and go to the properties.
 - b. Under the **Security** tab, click **Advanced settings** in the **Type of VPN** section, and enter the preshared key.



- c. Click **OK** twice to exit the connection properties.
4. Connect to the IPsec server.

Step 3. Apply the Installation to the Client Device

Once you are successfully connected, provision the device configuration to the client device. Be aware, that, for this procedure, the user must have been granted the appropriate access rights. For more information, see: [Provisioning Client Devices](#).

1. From the **Resources** tab of the client device, go to **Device Configuration**.
2. Tick the checkbox under the IPsec server entry.
3. Click **Provision** on the bottom of the page.

How to Configure Mobile Devices

To configure your mobile device to connect to the Barracuda SSL VPN, follow the instructions given in the relevant article section:

- [Configure an iOS Device](#)
- [Configure an Android Device](#)

- [Configure a Windows 8 RT Surface Tablet](#)
- [Configure a Windows Mobile Device](#)

Related Article

- [How to Configure IPsec](#)

Configure an iOS Device

The Barracuda SSL VPN will automatically make the configuration changes required on your iPhone or iPad. To configure the client device, complete the following steps:

1. In a web browser, go to the login page of the Barracuda SSL VPN; for example: <https://sslvpn.example.com/>
2. On your **RESOURCES > My Resources** page, you will see an **IPsec** or **PPTP** resource if the Barracuda SSL VPN is configured to accept L2TP/IPsec or PPTP connections.
3. Click on the **IPsec** or **PPTP** icon (either one will work). This will launch a mobile configuration profile which will prompt you to install it.
4. Select **Install**, and then select **Install Now**.
5. Enter your account name and password and click **Next**.
6. Click **Done**. The newly-created connection will appear in the **VPN** menu as well as in the main **Settings** menu.
7. Go to **Settings > General > Network > VPN > <VPN name>** to start the connection.

Configure an Android Device

To configure your Android device to connect to the Barracuda SSL VPN, complete the following steps:

1. On the Android device, tap **Settings > Wireless & Networks > VPN Settings > Add VPN**.
2. To configure an **L2TP/IPsec** connection, select **Add L2TP/IPsec PSK VPN** (for Preshared key) and configure only the following settings (for all other settings, accept the default values):
 - **VPN name** - A name for this connection (for example: *Sslvpn-ipsec*).
 - **Set VPN server** - The hostname or IP address of the Barracuda SSL VPN (for example: *sslvpn.example.com*).
 - **Set IPsec pre-shared key** - Select to enter the pre-shared key.
 - **Enable L2TP secret** - Clear this setting.
 - **DNS search domains** - Enter the default domain for the protected network (for example: *example.com*).
3. To configure a **PPTP** connection, select **Add PPTP VPN** and configure only the following settings (for all other settings, accept the default values):
 - **VPN name** - A name for this connection; for example: *Sslvpn-pptp*.
 - **Set VPN server** - The hostname or IP address of the Barracuda SSL VPN (for example: *sslvpn.example.com*).
 - **Enable Encryption** - Select to enable encryption of your PPTP session.
 - **DNS search domains** - Enter the default domain for the protected network (for example: *example.com*).
4. Select **Save**. The newly-created connection appears in the **VPN Settings** menu.

When you attempt a connection to the Barracuda SSL VPN, you are prompted for your username and password.

Configure a Windows 8 RT Surface Tablet

Edit Windows 8 RT Registry Entry

If both your remote computer and the Barracuda SSL VPN are behind a router that uses NAT (which is the most common scenario), you will have to edit the Windows 8 RT registry to allow access to an L2TP/IPsec server behind NAT-T devices.

To edit the registry entry on Windows RT, proceed as follows:

1. On the Microsoft Surface tablet, swipe in from the right edge of the screen, and tap the **Search** (magnifying glass) charm.
2. Type **regedit** and select it from the list.
3. Navigate to **Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent**.
4. On the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
5. Type **AssumeUDPEncapsulationContextOnSendRule**, and then press Enter.
6. Right-click **AssumeUDPEncapsulationContextOnSendRule**, and then click **Modify**.
7. In the **Value Data** box, set the value to 2.

8. Click **OK** and exit regedit.
9. Restart Windows 8 RT:
 - a. Swipe in from the right edge of the screen, and tap **Settings**.
 - b. Tap or click **Power**, and then tap or click **Restart**.

Create the IPsec Connection

Use the following steps to create the IPsec connection:

1. On the Microsoft Surface tablet, swipe in from the right edge of the screen, and tap the **Search** (magnifying glass) charm.
2. Type **VPN** to search for it in settings.
3. Select **Set up a virtual private network (VPN) connection**. This opens the **Create a VPN Connection** window in Desktop mode.
4. Enter the Barracuda SSL VPN IP address or host name, and enter a name for the connection.
5. Click **Create**. The Networks widget will appear and give you the option to connect. This is not going to work yet though as you have not yet entered the preshared Key. Press the icon to the right of the new connection until the **Context** menu appears.
6. Select **View Connection Properties**. The **Properties** will display in desktop mode.
7. Click the **Security** tab, and set the VPN type to **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)**.
8. Click **Advanced Settings**. Select **Use pre-shared key for authentication**, and enter the preshared key that your administrator gave to you and click **OK**.
9. On the **Security** tab:
 - a. Select **Allow these protocols**
 - b. Select **PAP**
 - c. Clear **MS-CHAP v2** (so only PAP is selected)
 - d. Click **OK**.

Launch SSL VPN

Use the following steps to launch SSL VPN:

1. On the Microsoft Surface tablet, swipe in from the right edge of the screen, tap the **Settings** (gear) charm, and then tap the currently connected network icon. The **Networks** list will display, and you will see the IPsec connection near the top.
2. Select that connection. Tap **Connect**. Enter your login credentials to access the Barracuda SSL VPN.

Configure a Windows Mobile Device

If you own a device running Windows Mobile complete the following steps:

1. On the Windows Mobile device, navigate to: **Settings > Connections > Add a new VPN server connection**.
2. Select **Make New Connection**, and then configure just the following (for all other settings, accept the default values):
 - **Name** - A name for this connection; for example: *Sslvpn-pttp*
 - **Hostname/IP** - The FQDN or IP address of the Barracuda SSL VPN; for example: *sslvpn.example.com*
 - **VPN type** - Select the desired VPN type (**IPSec/L2TP** or **PPTP**).
3. Select **Next**.
4. If **IPsec/L2TP** was chosen, then a screen will appear from which you must select **A pre-shared key** and enter the PSK for the Barracuda SSL VPN.
5. Then, select **Next**. The newly-created connection will appear in the **Connections** page, in the **VPN** tab.

Your username and password will be requested when a connection to the Barracuda SSL VPN is attempted.

How to Configure Remote Devices

As soon as the Barracuda SSL VPN is configured to allow remote access, you can setup a connection on a remote device. All you need to do is to make sure that you have the appropriate credentials, and that the system you want to use has the appropriate type of client (L2TP/IPsec) that will already come pre-installed on your device, in most cases.

In this article:

- [Configure a Windows 7 Client Device](#)
- [Configure a Windows 8 Client Device](#)
- [Configure a Mac OS X Client Device](#)

Related Article

- [How to Configure IPsec](#)

Configure a Windows 7 Client Device



The details of the following steps are specific to Windows 7, but can be adapted for other Windows versions such as XP and Vista by navigating to the corresponding feature on the system.

1. Log into the Barracuda SSL VPN. On your **RESOURCES > My Resources** page, you will see a **Barracuda IPsec** resource if the Barracuda SSL VPN has been configured to accept L2TP/IPsec connections.
2. Click on the **Barracuda IPsec** configuration tool. The Barracuda SSL VPN Agent will automatically create and configure an L2TP/IPsec VPN connection on your Windows system.



Configuring the IPsec settings may require administrator privileges on your system.

3. Once the configuration (and possible reboot) has completed, navigate to **Control Panel > Network and Internet > Network and Sharing Center**.
4. Select **Connect to a network**, click on the **Barracuda IPsec** entry, and click **Connect**.
5. On the connect dialog, select **Properties** and go to the **Security** tab.
6. Click **Advanced settings**, and from the **L2TP** tab:
7. Select **Use preshared key for authentication**.
8. In the **Key** field, enter the PSK for the Barracuda SSL VPN.
9. Click **OK** to return to the **Security** tab.
10. Click **OK** to save your settings and return to the connect dialog.
11. To log in, enter the following information:
 - **User name** - The account name for the connecting user; for example; *psmith*
 - **Password** - The password for the username specified above.
12. Click **Connect**.

Configure a Windows 8 Client Device

For Windows 8 systems, the required configuration changes are automatically made. To verify that your system makes the changes automatically:



Known Issue: It is necessary for users to manually enter the PSK in the IPsec configuration.

1. Launch the browser on your remote system and log into the Barracuda SSL VPN.
2. On your **RESOURCES > My Resources** page, you will see a **Barracuda IPsec** resource (an administrator can change the name of this resource).
3. Click on the **Barracuda IPsec** icon. This launches the Barracuda SSL VPN Agent and configures the VPN connection on your Windows 8 system.

If these instructions do not work, your Barracuda SSL VPN is probably running an older version. Continue with the rest of this article.

Windows 8 for IPsec

1. Launch the browser on your remote system and log into the Barracuda SSL VPN. On your **RESOURCES > My Resources** page, you will see a **Barracuda IPsec** resource if the Barracuda SSL VPN has been configured to accept L2TP/IPsec connections.
2. Click on the **Barracuda IPsec** icon. This launches the Barracuda SSL VPN Agent and asks you to configure the L2TP/IPsec VPN connection on your Windows 8 system.
3. On the **Connect** dialog that appears:
4. Click **Properties**.
5. In the **General** tab, enter the IP address or host name of the Barracuda SSL VPN.
6. In the **Security** tab, select *Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)* and click **Advanced settings**.
7. On the **Advanced Properties** dialog, select **Use preshared key for authentication** and enter the preshared key given to you by your IT administrator.
8. Click **OK** two times.
 - If both your remote computer and the Barracuda SSL VPN are behind a router that uses NAT (most likely scenario), you will

have to edit the Windows 8 registry to allow access to an L2TP/IPsec server behind NAT-T devices:

- a. Press the **Windows** key on your keyboard.
- b. Type **regedit** and then run the regedit app.
- c. Navigate to **Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent**.
- d. On the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
 - i. Type **AssumeUDPEncapsulationContextOnSendRule**, and then press **Enter**.
 - ii. Right-click **AssumeUDPEncapsulationContextOnSendRule**, and then click **Modify**.
 - iii. In the **Value Data** box, set the value to 2
 - iv. Click **OK** and exit regedit.
 - v. Restart Windows.
9. Once the restart has completed, launch your browser and log into the Barracuda SSL VPN again.
10. On your **RESOURCES > My Resources** page, click the **Barracuda IPsec** icon.
11. On the connect dialog, enter the following information and click **Connect**:
 - **User name** – The account name for the connecting user; e.g., **psmith**
 - **Password** – The password for the username

You should be able to connect to the Barracuda SSL VPN and access your resources.

Configure a Mac OS X Client Device

1. On the remote device, navigate to **System Preferences > Network**.
2. Click **+** to add a new service.
3. On the dialog that appears, enter the following:
 - **Interface** - Select **VPN** from the list.
 - **VPN type** - Select **L2TP over IPsec**.
 - **Service name** - Name of your selection.
4. Select the service you created. (The status will show as **Not Configured**.)
5. Enter the following:
 - **Server Address** - The external IP address or the URL of your Barracuda SSL VPN.
 - **Account Name** - Your account name for authentication (for example: LDAP or Active Directory user name).
6. Click **Authentication Settings...**
7. Enter the following:
 - **Password** - Your account password.
 - **Shared secret** - Provided to you by your IT administrator.
8. Click **OK**.
9. To connect to the Barracuda SSL VPN, highlight the service and click on **Connect...**

How to Configure PPTP

PPTP, or Point-to-Point Tunneling Protocol, enables authorized mobile devices, including smartphones, to access your organization's network. To connect to your Barracuda SSL VPN using PPTP, your **remote device** must have an appropriate VPN client that supports the desired authentication protocol, preferably MSCHAPv2.



As of 2012, PPTP is no longer considered secure. It is highly recommended that you switch away from PPTP.

In this article:

- [Before you Begin](#)
- [Step 1. Enable PPTP Server](#)
- [Step 2. Create a PPTP Connection](#)
- [Step 3. Download the Configuration to the Client Device](#)

Before you Begin

- On your organization's firewall, allow authentication traffic to and from the Barracuda SSL VPN. TCP over port 1723 and GRE (IP Protocol 47) forwarded to the Barracuda SSL VPN for PPTP connections to function.

Step 1. Enable PPTP Server

On the Barracuda SSL VPN, configure PPTP to allow your remote users to authenticate and connect to the protected network.

1. Log into the [SSL VPN Web interface](#).
2. Navigate to the **RESOURCES > PPTP Server** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Create PPTP Server** section, enter a descriptive name for your PPTP server.
5. In the **IP Range Start/End** fields, enter the first and last IP address of the DHCP range that should be assigned to remote systems connecting via PPTP.



This IP range must reside in the network range that is configured in the **Basic IP Configuration** section of the appliance interface, and **MUST NOT** be part of any other DHCP range on your LAN.

6. From the **Policies** list, select the available policies that you want to apply to the PPTP server, and add them to the **Selected Policies** list.
7. Click **Add**.

The PPTP Server is now created and appears in the **PPTP Server** section. You can test the configuration by clicking the **Launch** link associated with the entry.

Step 2. Create a PPTP Connection

On your remote device, create a PPTP connection to the Barracuda SSL VPN.

1. Log in to the Barracuda SSL VPN on the client device.
2. Go to the **Resources** tab.
3. From **My Resources**, select the PPTP server and click to connect.

Step 3. Download the Configuration to the Client Device

For more information, see: [Provisioning Client Devices](#).

1. From the **Resources** tab of the client device, go to **Device Configuration**.
2. Tick the checkbox for the PPTP server entry.
3. Click **Provision** on the bottom of the page.

How to Configure Profiles

Creating profiles allows the administrator to define specific settings for the general working environment of the system. Settings in a Profile can affect the timeouts of a user session, change the default view for resources (icons or lists) or also affect agent timeouts and proxy settings. If multiple profiles are configured users can select different profiles when logging in, or the administrators can manage default environment settings for users preselecting a matching profile. A default profile always exists and cannot be deleted.

Step 1. Create a Profile

1. Log into the [SSL VPN web interface](#).
2. Go to the **RESOURCES > Profiles** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Create Profile** section, select the database, for which you want to apply the profile from the **User Database** list.
5. Enter a unique name for the profile in the **Name** field.
6. From the **Policies** list, select the policies to associate with this profile and click **Add >>** to add them to the **Selected** area on the right.
7. Click **Add** to create the policy.

Step 2. (Optional) Configure Additional Profile Settings

The **Edit Profile** window lets you configure additional details if required, such as timeouts and local proxy settings.

1. To edit the profile settings, click the **Edit** link next to the profile in the **Profiles** list.
2. Modify the settings as required. The session parameters affect how the active session behaves and includes for example cache behavior and inactivity timeout.
3. Click **Save Changes**.

Users who are granted the appropriate permissions can create and manage their own profiles. For example, a user might configure a home profile which is configured for use when working from home and another called *On-site* which could be used for when the user is on a customer site.

Provisioning Client Devices

This functionality is supported on client devices running Microsoft Windows, iOS and Mac OS X 10.7 and above and requires Barracuda SSL VPN firmware version 2.4.0.9 or newer

The Device Configuration feature allows you to provision resources and other settings configured on the Barracuda SSL VPN directly on a user's device. When logged in, the user will see resources and settings on their **RESOURCES > Device Configuration** page, depending on what resources you make available to them and the operating system of the device. There they can select the resources to be provisioned and where they should be located on the device, for example, in a folder on the Desktop.

Before you Begin

For the user to be able to see the **RESOURCES > Device Configuration** page, the following conditions must be met:

- The user must have the *Personal Access Right/Device Configuration View Access Right*.
- There must be a accessible resource on the client to be provisioned.
- For the items: client certificates, mail settings, Exchange ActiveSync settings, and LDAP settings, the corresponding option on the **RESOURCES > Configuration** page must be set to allow the provisioning.

Grant Access to Users

Follow these instructions to grant users the *Personal Access Right/Device Configuration View Access Right*:

1. Log into the [SSL VPN web interface](#).
2. Verify that you have selected the correct user database on the top right of the page.
3. Go to the **ACCESS CONTROL > Access Rights** page.
4. In the **Create Access Right** section, select the relevant database from the **User Database** drop-down list.
5. Select **Personal Right**.
6. Enter a descriptive **Name** for this access right.
7. In the **Available Rights** list, select *Device Configuration View* and click **Add >>**.
8. In the **Available Policies** list, select the policies for which provisioning should be enabled and click **Add**.
9. Click **Add**.

On the **RESOURCES > Configuration** page, in the **Device Configuration** section, you can configure whether the non-resource items (certificate, mail settings, exchange, LDAP) can be provisioned.

Windows Devices

This table shows the types of items that can be provisioned to Windows devices.

Item Type	Description
• Applications • Web Forwards • Audit Reports • Network Places • SSL Tunnels	All of these resources, if available to the user on their device, can be provisioned as shortcuts that will immediately launch the appropriate resource when selected. Whether they appear or not depends on the user's access rights and whether they are applicable for the device (SSL tunnels and tunneled web forwards will not be available on iOS devices because they require the agent). The settings for the resource are provisioned only as shortcuts (an URL to the Barracuda SSL VPN and the appropriate icon).
Mapped Drives	If the user has access to at least one Network Place resource that has an associated drive mapping, a shortcut will be provisioned to the device that will initiate the drive mapping process.
Client Certificates	Installs the selected client certificate into the Windows keystore. Certificates are taken from the ADVANCED > SSL Certificates page (client certificates for the user only).
IPsec Settings	Creates a VPN connection on the device using the relevant IPsec settings configured on the RESOURCES > IPsec Server page.

PPTP Settings	Creates a VPN connection on the device using the relevant PPTP settings configured on the RESOURCES > PPTP Server page.
----------------------	---



Known Issue: The preshared key has to be entered manually by the user for PPTP and L2TP/IPsec connections on Windows devices.

iOS / Mac OS X Devices

This table shows the types of items that can be provisioned to iOS and Mac OS X (10.7 and above) devices.

Item Type	Description
Mail Settings	Creates an email account on the device using a variety of settings stored in the Barracuda SSL VPN. The email address is from the user account. The server details are found on RESOURCES > Configuration > Mail Checking for inbound settings and BASIC > Configuration > SMTP for outbound. The username and password for authenticating with the SMTP server are also taken from the same place, but for inbound mail they are taken from the user attributes for mail checking (ACCOUNT > Attributes > Mail Checking).
Exchange Settings	The remote device is configured to use the Barracuda SSL VPN to proxy the connection.
LDAP Settings	For users authenticated with the Barracuda SSL VPN using LDAP or OpenLDAP, the settings from the user database and user account will be provisioned to the device.
• Applications • Web Forwards • Audit Reports • Network Places • SSL Tunnels	All of these resources, if available to the user on their current device, can be provisioned as Web Clip shortcuts. Whether these resources appear depends on the user's access rights and whether they are applicable for the client device (SSL tunnels and tunneled Web Forwards will not be available on iOS devices because they require the agent). These items can be provisioned in the form of a profile installed on the device. The remote user can specify the name of the profile on the RESOURCES > Device Configuration page.
Client Certificates	Installs the selected client certificate onto the device. Certificates are taken from the ADVANCED > SSL Certificates page (client certificates for the user only).
IPsec Settings	Creates a VPN entry on the device using the relevant IPsec settings configured on the RESOURCES > IPsec Server page. The user will be prompted for their password when installing a profile containing IPsec settings.
PPTP Settings	Creates a VPN entry on the device using the relevant PPTP settings configured on the RESOURCES > PPTP Server page. The user will be prompted for their password when installing a profile containing PPTP settings.

By default, all shortcuts created are added to the user's Desktop, Start Menu and web browser, in a sub-folder whose name matches that of the Barracuda SSL VPN. If the web browser option is selected, the user will be prompted from the Barracuda SSL VPN agent asking which browsers to provision shortcuts to. When the installation is completed, the agent will add the bookmarks to all profiles defined within those browsers.

Bookmark Aliases

When shortcuts are created, they point at URLs on the Barracuda SSL VPN. For example, the shortcut looks like <https://sslvpn.example.com/web-forward/jira>. By default, the Barracuda SSL VPN will attempt to generate an alias from the resource name when it is created. This will strip out any

illegal characters and append a numeric value if the alias already exists. You can specify these aliases on the edit pages of the respective resources. To disable aliasing, go to **RESOURCES > Configuration > Bookmarking**. In this case, the provisioned shortcuts will instead refer to the verbose URL.

Advanced Configuration

In addition to the general setup and configuration utilities, the Barracuda SSL VPN provides an advanced configuration area that lets you specify extended settings such as advanced system wide User and Policy attributes, Messaging and the Barracuda SSL VPN Agent that secures unencrypted connections from the client device to the SSL VPN.

In this Section:

- [Attributes](#)
- [Messaging](#)
- [Agents](#)

Attributes

Attributes are system wide dynamic variables to store either user or policy information. After defining attributes the variables can be used in every configuration where dynamic expressions can be used.

User Attributes

The system comes with a set of default user attributes, which can be extended by the administrator. User Attributes can be used for user specific answers to security questions or customization for Resources. Custom user attributes can be used in every context where dynamic expressions are allowed.

Policy Attributes

Policy attributes are variables which are set for policies. Once set these attributes are valid for all users attached to that policy. You can run the same resource with different policies, each policy setting the policy attributes to a different value. For Example: if the engineering group is using a different Exchange server from Sales or Marketing you can define a policy variable with the Exchange server name. When an engineer uses the Exchange resource, the Barracuda SSL VPN uses the server name stored in the policy attribute to connect to the correct server.

Messaging

Messaging allows the user to send messages either to an individual or groups.

Create a Message

To create and send a message within the Barracuda SSL VPN,

1. Log into the [SSL VPN web interface](#).
1. Go to the **Advanced > Messaging** page.
2. Verify that you have selected the correct user database on the top right of the page.
3. From the **User Database** drop down list, select the database where the users are located, or select *Global View* to list all users.
4. In the **Subject** field, enter the subject for the message.
5. From the **Delivery Method** drop down list, select the delivery method to use:



The list varies depending on whether the method is configured or not. If you want to use email, you must first configure the SMTP settings. If you want to use SMS over email, configure the SMS settings on the **ACCESS CONTROL > Configuration** page.

- **First** - Send the message via the first available delivery method. This option is useful if the messaging configuration is frequently altered or the recipients do not mind how they are contacted.
 - **All** - Send the message via all available delivery methods. This guarantees that individuals will always receive a message in some way, but it means that the recipients may get multiple copies of the message.
 - **Agent** - Send the message via the SSL VPN Agent to only those recipients who are currently running the SSL VPN Agent. This is useful if, for example, you want to warn that you are shutting down the service for maintenance.
 - **Email** - Send the message via email.
 - **SMS over Email** - Send the message to mobile phones using the SMS gateway service.
6. If the message should be treated as urgent, select **Urgent** to place it at the front of the message queue.
 7. If the message should be treated as secure, select **Secure**, to not display the message contents within the Audit Log or Reports.

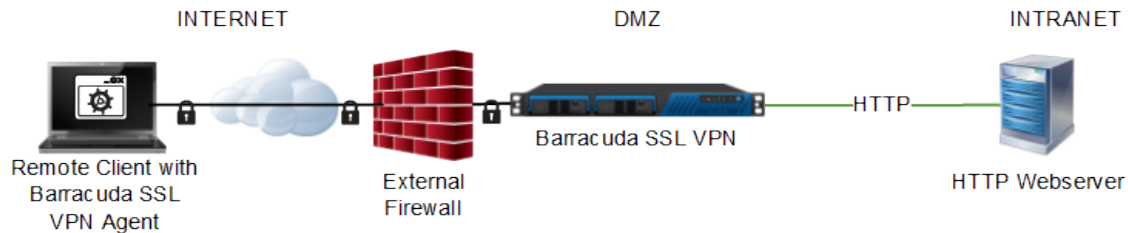
8. Enter your message in the **Content** field.
9. Select one or more Accounts, Groups or Policies to which the message will be sent.
10. Click **Send** to save this entry.

An entry for this message will be displayed in the **Messages** section below. By default, all available messages are listed in alphabetical order. To display only the messages that begin with certain characters, enter the desired text in the area on the left, and click **Apply Filter**.

Agents

There are two agents for the Barracuda SSL VPN. The Barracuda SSL VPN Agent which secures unencrypted connections from the client computer to the SSL VPN and the Server Agent which creates a SSL tunnel to relay traffic for resources which can not be directly accessed by the SSL VPN. Both Agents create a SSL tunnels to the Barracuda SSL VPN, acting as a transparent proxy.

SSL VPN Agent

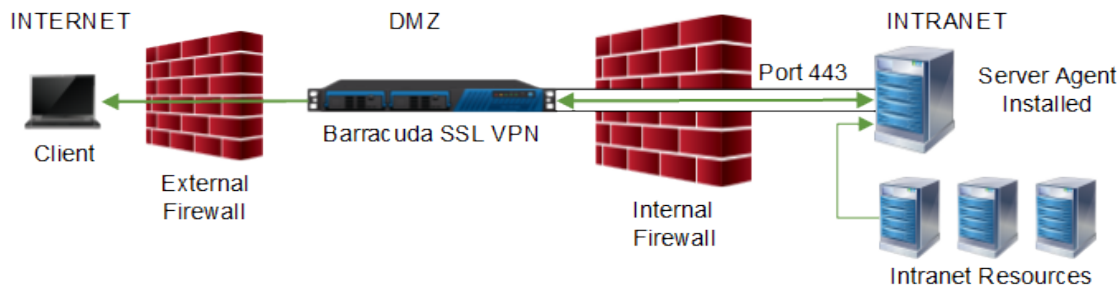


The Barracuda SSL VPN Agent is used to tunnel unencrypted connections. The traffic is intercepted and rerouted by the SSL VPN Agent installed on the client computer and then sent through a SSL encrypted tunnel to the Barracuda SSL VPN.

i The SSL tunnel creates a secure tunnel into your network. It is important that users log out and do not leave their session unattended. The tunnel will disconnect, if it is inactive for a configurable amount of time.

For more information, see [How to Configure the SSL VPN Agent](#).

Server Agent

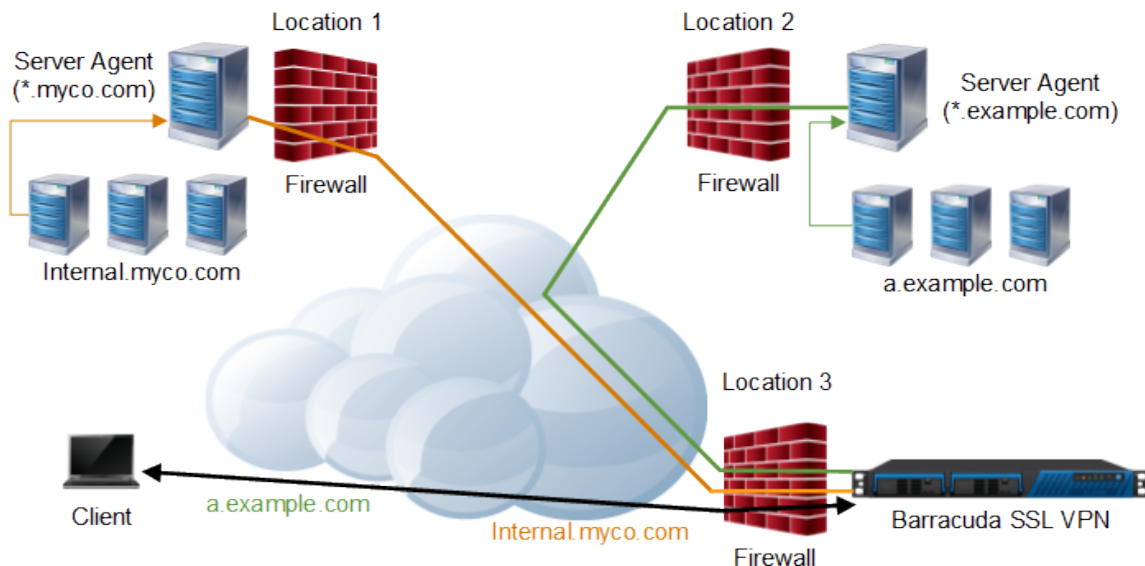


The Barracuda Server Agent is installed inside of a network, which can not be reached directly by the Barracuda SSL VPN. The Server Agents initiates a HTTPS connection from inside of the network, using port 443. It then waits for requests from the SSL VPN and forwards traffic for the local resources. For example if you want to make the internal company wiki available via SSL VPN, the Server Agent is installed on a computer or server in the same network. It will then act as a transparent proxy, relaying the information to the SSL VPN which delivers the content to the client. The SSL VPN can use multiple Server Agent in different networks, using routes containing host patterns (e.g., *.example.com) to decide which Server Agent to contact for a particular resource. The whole process is completely transparent to the user.

For more information, see [How to Configure a Server Agent](#).

How to Configure a Server Agent

The Barracuda Server Agent is used to proxy traffic for resources located in a network which can not be reached directly by the Barracuda SSL VPN. For this example the client will request a web resource hosted on the *a.example.com* server in the intranet. The Barracuda SSL VPN will use the server agent installed on one of the local servers in the network to connect to the *a.example.com* server and forward the traffic to the client.



In this article:

- [Step 1. Install the Server Agent Client](#)
- [Step 2. Authorize Server Agents](#)
- [Step 3. Create Routes](#)

Step 1. Install the Server Agent Client

For every network you want to connect to the Barracuda SSL VPN with a Server Agent, install the client on a system in the network that can reach all the resources you want to access via the SSL VPN.

1. Log into the [SSL VPN web interface](#).
2. Open the **Manage System > ADVANCED > Server Agents** page.
3. In the **Download Clients** section, click on the download link for your operating system.

After installing the software package, enter the IP address and authentication information for your Barracuda SSL VPN. The Server Agent will automatically register with the Barracuda SSL VPN. The Server Agent is now listed in the **Agents** section on the **Manage System > ADVANCED > Server Agents** page.

Step 2. Authorize Server Agents

You need to authorize the Server Agents after the initial connection.

1. Log into the [SSL VPN web interface](#).
2. Open the **Manage System > ADVANCED > Server Agents** page.
3. In the **Agents** section, locate the Server Agent with the red indicator icon and click **More**.
4. Select **Authorize**.

The indicator icon is now green. If the indicator icon is yellow, the Server Agent is offline or blocked.

Step 3. Create Routes

Routes are used to tell the Barracuda SSL VPN which Server Agent is responsible for a particular resource. You can define multiple routes for every Server Agent.

1. Log into the [SSL VPN web interface](#).
2. Open the **Manage System > ADVANCED > Server Agents** page.
3. In the **Create Route** section, enter the following information:
 - **Name** – Enter a name.
 - **Host Pattern** – Enter a host pattern. This can be an IP address or a domain. Wildcards are allowed. E.g., 10.0.100.* or *.myco.com
 - **Port Pattern** – Enter a single port, or port range that applies to the resources using this server agent. E.g., 800*
 - **Server Agent** – Select the Server Agent from the list.
4. Click **Add**.

The routes are now visible in the **Routes** section. If you want to move a route to a different Server Agent, edit the Server Agent configuration in the **Agents** list.

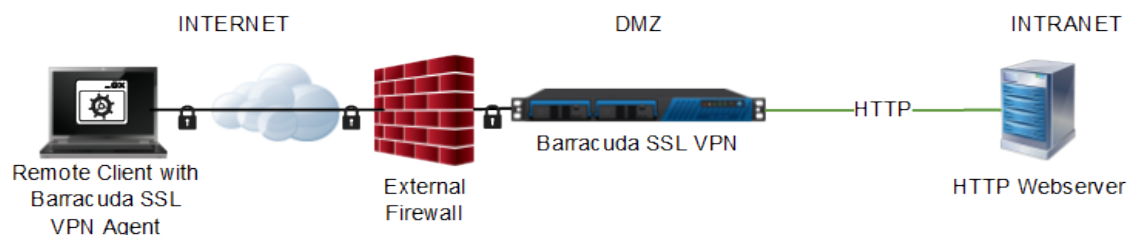
How to Configure the SSL VPN Agent

The SSL VPN Agent is a small client installed on the client computer to tunnel unencrypted connections. The traffic is intercepted and rerouted through a SSL tunnel created by the SSL VPN Agent.

i The SSL tunnel creates a secure tunnel into your network. It is important that users log out and do not leave their session unattended. The tunnel will disconnect, if it is inactive for a configurable amount of time.

Related Articles

- [How to Configure Profiles](#)



Executing Resources from the Barracuda SSL VPN Agent

The SSL VPN Agent is launched by a small applet placed on all pages that require access to the SSL VPN client. When the Agent has been started the Barracuda SSL VPN Agent taskbar icon is visible. While the SSL Agent is running, you can start all your resources from the icon in the taskbar. The SSL VPN Agent terminates when the browser session is closed or the user logs out.

Enable the SSL VPN Agent on Login

You can [configure the Profile](#) used for a user group to start the SSL VPN Agent automatically when the user logs in. All Resources can now be started from the taskbar. The SSL VPN Agent is terminated when the users session ends, by logging out or closing the browser.

For more information, see [How to Configure Profiles](#).

Monitoring

The Barracuda SSL VPN incorporates hardware and software fail-safe mechanisms that are indicated via notifications and logs. You can inspect the logs to see what is happening with traffic. SNMP monitoring and traps for the Barracuda SSL VPN model 380 and larger are supported.

The following articles explain the tools and monitoring tasks that you can use to track user numbers and system performance.

In this Section

- [Basic Monitoring](#)
- [Notifications](#)
- [SNMP](#)

Basic Monitoring

The Barracuda SSL VPN lets you monitor the performance of your Barracuda SSL VPN system including traffic and policy details, the subscription status of Energize Updates, as well as performance statistics, including CPU temperature and system load when using a hardware appliance.

In this article:

- [Status and Performance](#)
- [Session Monitoring](#)
- [Viewing Event Logs](#)
- [System Tasks Overview](#)

- [Web Interface Syslog](#)
- [SNMP Support](#)

Related Article

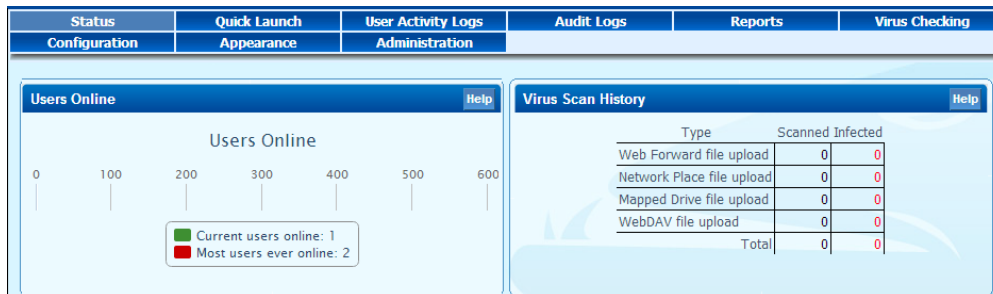
- [SNMP](#)

Status and Performance

The **Status** page displays information about the current status of the Barracuda SSL VPN server for the last 24 hours.

1. Log into the [SSL VPN Web interface](#) .
2. Go to the **BASIC > Status** page.

The status information is displayed as follows:



The graphs displayed on the **Status** page provide information about session types, user activity, resources and traffic sent through the Barracuda SSL VPN.

Session Monitoring

The **Sessions** screen displays all active sessions of users that are currently logged in.

1. Log into the [SSL VPN Web interface](#) .
2. Go to the **ACCESS CONTROL > Sessions** page.

Sessions Help					
Apply Filter Reset					
User	User Database	Session Type	IP Address	Logon Time	Actions
ssladmin	Super Users	Browser	10.0.10.2	2013-12-03 04:41:35	Log Off
ssladmin	Super Users	Browser	10.0.10.2	2013-12-03 04:39:38	Log Off

Expand a session by clicking + where applicable displays further details like launch time and traffic information. The **Log Off** option disconnects the user.



The **User Database** column is only visible when the **Global View** database is selected.

Viewing Event Logs

The **User Activity Logs** page displays all user-level events, whilst the **Audit Logs** page lists all system-level events. To access the event logs screens,

1. Log into the [SSL VPN web interface](#) .
2. Go to the **BASIC > User Activity Logs** page. For audit logs, select **BASIC > Audit Logs** .

Audit Logs Help						
Filter: None Pattern: + Apply Filter Reset						
Date	Event	Description	User Database	Username	Host Address	State
2013-12-03 03:26	Remote Assistance Request Deleted	Title 'testuser requires assistance' requested for 'Test User' between '*' and '*'	Global View	ssladmin	10.0.10.2	Successful
2013-12-03 01:43	Attached Policy To Resource	Attached Policy 'Everyone' To Resource 'Request Remote Assistance'	Global View	ssladmin	10.0.10.2	Successful

Click on the header of a column to sort by that column. You can also filter the list by selecting a category from the **Filter** drop down list.

 The **User Database** column is only visible when the **Global View** database is selected.

System Tasks Overview

The **Task Manager** page provides a list of tasks that are in the process of being performed, and displays any errors encountered when performing these tasks, for example: imports of historical emails, exports of archived messages and configuration restoration. If a task takes a long time to complete, you can click **Cancel** next to the task name and then run the task at a later time when the system is less busy. The **Task Errors** section will list an error until you manually remove it from the list. To access the **Task Manager** page,

1. Log into the Barracuda SSL VPN Web interface as the *admin* administrative user.
2. Go to the **ADVANCED > Task Manager** page.

Web Interface Syslog

Supporting both IPv4 and IPv6 addressing with port numbers, the Syslog feature makes it possible to send all log information to a syslog server. To configure syslog settings,

1. Log into the [Administrative web interface](#).
2. Go to the **ADVANCED > Syslog** page.

To monitor the Web syslog output, containing information regarding various events such as user login activities and configuration changes made from the administrative interface of the Barracuda SSL VPN,

1. Log into the [SSL VPN web interface](#).
2. Go to the **ADVANCED > Syslog** page.
3. Click **Monitor Web Syslog**.

SNMP Support

The Barracuda SSL VPN offers the ability to configure the monitoring of various settings through SNMP, including traffic and policy statistics. For instructions on how to configure SNMP settings on the Barracuda SSL VPN, see [SNMP](#).

Notifications

Notifications are configurable messages that are sent to users to inform them of important events happening on the Barracuda SSL VPN. Notifications are sent by email, agent or SMS over email. You can configure who should be notified for every event.

Create a Notification

Related Article
• SNMP

If you want to be informed when a certain event occurs on the Barracuda SSL VPN, you need to create a notification:

1. Log into the [SSL VPN web interface](#).
2. Open the **ADVANCED > Notifications** page.
3. In the **Create Notification** section, select the **User Database**.
4. Enter a **Name**.
5. Select the **Event State**.
6. Double-click all events you want to associate with this notification in the **Available Events** list.

7. Select which type of user you want to receive the notification. If you select **Administrative User** all administrator who have sufficient rights to act on the event will receive the notification.
8. Click **Add**.

The notification is now listed in the **Notifications** section below.

Notifications Help			
Apply Filter Reset			
Name	User Database	Delivery Method	Actions
Failed Logon	Global View	Email	Edit Copy Delete More ..
Failed NAC Authentication	Global View	Email	Edit Copy Delete More ..
Remote Assistance Notifications	Global View	Email	Edit Copy Delete More ..
Server Shutdown Scheduled	Global View	Agent	Edit Copy Delete More ..

If you want to modify a notification after it has been created, or define the recipients in a more granular way, click **Edit** next to the notification, make the necessary changes and save your settings. To remove a notification, click **Delete**.

SNMP

All Barracuda SSL VPNs model 480 and larger offers the ability supply various information to Network Management Systems via SNMP. Both SNMP version 2c and 3 are supported. Barracuda Networks recommends using SNMP v3 as it is more secure.

In this article:

- [SNMP v2](#)
- [SNMP v3](#)
- [Configure SNMP v2](#)
- [Configure SNMP v3](#)
- [Enable SNMP Traps](#)

SNMP v2

Related Article
• Basic Monitoring

- IP address (range) from which the Network Management System will contact the Barracuda SSL VPN SNMP service.
- SNMP community string.

SNMP v3

- User and password to authenticate the NMS.
- Authentication Method (supported encryption methods).
- Allowed IP address or range for the Network Management System.

Configure SNMP v2

1. Log into the [Administration interface](#).
2. Open the **ADVANCED > Administration** page.
3. In the **SNMP Manager** section, configure the following settings:
 - **Enable SNMP Agent** – Select Yes.
 - **SNMP Version** – Select **v2c**.
 - **SNMP Community String** – Enter a password to authenticate the SNMP server.
 - **Allowed SNMP IP/Range** – Enter the IP addresses or range from which the Barracuda SSL VPN should accept SNMP queries.
4. Click **Save Changes**.

Configure SNMP v3

1. Log into the [Administration interface](#).
2. Open the **ADVANCED > Administration** page.
3. In the **SNMP Manager** section configure the following settings:
 - **Enable SNMP Agent** – Select Yes.
 - **SNMP Version** – Select **v3**.
 - **User** – Enter a username.

- **Password** – Enter a password.
 - **Authentication Method** – Select the authentication method supported by your network management software. E.g., SHA
 - **Encryption Method** – Select the encryption method supported by your network management software. E.g., AES
 - **Allowed SNMP IP/Range** – Enter the IP addresses or range from which the Barracuda SSL VPN should accept SNMP queries.
4. Click **Save Changes**.

Enable SNMP Traps

If you want your Barracuda SSL VPN to send SNMP traps to the network management system add the IP address:

1. Log into the [Administration interface](#).
2. Open the **ADVANCED > Administration** page.
3. In the **SNMP Traps** section, add the IP address of the network management system.
4. Click **Save Changes**.

Maintenance

The following article section describes in detailed steps how to configure and restore backups of the Barracuda SSL VPN configuration and explains the procedure of firmware updates.

In this Section

- [How to Configure Automated Backups](#)
- [Restore from Backups](#)
- [Update Firmware](#)
- [How to Update the Firmware in a High Availability Cluster](#)

How to Configure Automated Backups

It is recommended to always have working backups of your appliance. In case of a hardware failure or system misconfiguration the backup files can be used to quickly restore the appliance to working order. The administrator can configure how many backups are saved to a SMB share, FTP or FTPS server.

Related Article

- [Restore from Backups](#)

Configure Automatic Backups

1. Log into the [Administrative web interface](#).
2. Open the **BASIC > Backups** page.
3. In the **Automated Backups** section, complete the following tasks:
 - Configure the remote server where the backups are stored. You can choose between SMB and FTP servers. You can verify the connection to the remote storage by clicking **Test Backup Server**.
 - Select the type of backups you want to create and set the time.
4. Click **Save Changes**.

Restore from Backups

You can restore the Barracuda SSL VPN from a backup file you previously created. If you did a complete backup or just a backup up of the Appliance or SSL VPN configuration you can do a full or partial restore.

Complete Restore for the Barracuda SSL VPN

Related Article

- [How to Configure Automated Backups](#)

1. Open the **BASIC > Backups** page.
2. In the **Restore Backups** section, select the **Restore From:** backup file source. Select **smb** to restore from a network share, or local if you have the backup files on your local computer.
3. Click **Browse**.

Restore Backups

Help

Note: Uploaded backups must be confirmed to take effect and will overwrite the current configuration.

Restore From:

SMB

Browse

Select the destination where the desired backup file is stored.

Show All Backups: ☐ Yes ☒ No

Include all backups on the server, not limiting to backups saved by this appliance.

- Select the backup file and click **Open**.
- After the upload has completed click **Finish**.

Loading in progress

Your backup file has been loaded successfully.

Finish

- On the top of the page select the **Components** you want to restore. For a complete restore select **Configuration** and **SSL VPN Configuration/Logs**.
- Click **Restore Now**.

RESETTING ... Please Wait

Wait while the Barracuda SSL VPN restored the configuration from the selected backup files. You will be redirected to the login screen once the restore process has been completed.

Update Firmware



Read the entire article before upgrading your Barracuda SSL VPN.

The Barracuda SSL VPN firmware is available as:

- General Release (GA)** – The latest generally available firmware from Barracuda Central.
- Early Release (EA)** – The newest version of firmware available for early access from Barracuda Central.

Related Article

- [How to Update the Firmware in a High Availability Cluster](#)

General Release

GA firmware is the final and fully tested firmware version. Barracuda Networks highly recommends that you download the GA release as soon as it is available to take advantage of important new features and fixes.

Early Release

EA firmware is available for early adopters who wish to test the latest firmware from Barracuda Networks, or who have a specific need for early access, such as a new feature or bug fix that would be beneficial to your environment

Before downloading the EA firmware release, consider the following:

- This is a one-way upgrade; reverting to an earlier firmware version is not recommended;
- Once you install the EA firmware, you must update each point release up to the final GA release to take advantage of latest fixes.

Update your Barracuda SSL VPN Firmware



The appliance will reboot when the firmware update is applied. Make sure you do not unplug or manually reset your Barracuda SSL VPN during the update process unless instructed to do so by [Barracuda Networks Technical support](#).

1. Log into the [Appliance web interface](#).
2. Open the **ADVANCED > Firmware Update** page.
3. If a new firmware version is available, click **Download Now** next to the version (GA or EA) you want to upgrade to.
4. Click **Apply Update** after the update has been downloaded to the appliance.

The Barracuda SSL VPN will reboot and perform the update. This may take up to 20 minutes.

How to Update the Firmware in a High Availability Cluster

Special care needs to be taken when updating the firmware in a high availability cluster. To avoid synchronization errors and inconsistencies, it is necessary to remove all units from the cluster and update each one individually. After the update, recreate the cluster. Each Barracuda SSL VPN system in a cluster must be on exactly the same firmware version, so plan to update the units at the same time.



It is strongly recommended that you create a back up (**ADVANCED > Backup**) before proceeding.

Related Articles

- [Virtual Systems](#)
- [Update Firmware](#)
- [High Availability Deployment](#)

Step 1. Remove all Units from the Cluster

On each system in the cluster, proceed as follows:

1. Go to the **ADVANCED > Linked Management** page and delete the **Cluster Shared Secret**. You will have to log in again.
2. If you are using a Simple High Availability Cluster:
 - a. Navigate to **ADVANCED > Linked Management**.
 - b. In the **Simple High-Availability** section, clear the value of the IP address if it exists (you may only need to do this on the first system).
3. Log back in.
4. Navigate to **ADVANCED > Linked Management**.
5. Delete all entries from the list of clustered systems, except the unit you are logged in to.

Step 2. Update the Firmware

Update one unit first to verify that the upgrade applies successfully and the Barracuda SSL VPN is operating as expected. Then update the rest of the systems.

1. Go to the **ADVANCED > Firmware Update** page and download the new firmware.
2. Click **Apply** to update the system.
3. After the system reboots, verify that the firmware has been applied successfully and is operating as expected.

Step 3. Recreate the Cluster

Choose one unit as the primary unit. All other systems in the cluster will pull the configuration from this unit. Complete the following steps for all units to recreate the cluster.

1. Log into the [SSL VPN web interface](#).
2. Open the **ADVANCED > Linked Management** page.
3. Enter the **Cluster Shared Secret**.
4. Click **Save Changes**.

5. If the unit is not the primary unit:
 - a. Navigate to **ADVANCED > Linked Management**.
 - b. In the **Clustered Systems** section enter the IP address of the primary unit and click **Add System**.
 - c. Click **Join Cluster**.



The configuration of this unit will now be overwritten with the configuration from the primary unit.

Limited Warranty and License

Limited Warranty

Barracuda Networks, Inc., or the Barracuda Networks, Inc. subsidiary or authorized Distributor selling the Barracuda Networks product, if sale is not directly by Barracuda Networks, Inc., ("Barracuda Networks") warrants that commencing from the date of delivery to Customer (but in case of resale by a Barracuda Networks reseller, commencing not more than sixty (60) days after original shipment by Barracuda Networks, Inc.), and continuing for a period of one (1) year: (a) its products (excluding any software) will be free from material defects in materials and workmanship under normal use; and (b) the software provided in connection with its products, including any software contained or embedded in such products will substantially conform to Barracuda Networks published specifications in effect as of the date of manufacture. Except for the foregoing, the software is provided as is. In no event does Barracuda Networks warrant that the software is error free or that Customer will be able to operate the software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the software or any equipment, system or network on which the software is used will be free of vulnerability to intrusion or attack. The limited warranty extends only to you the original buyer of the Barracuda Networks product and is non-transferable.

Exclusive Remedy

Your sole and exclusive remedy and the entire liability of Barracuda Networks under this limited warranty shall be, at Barracuda Networks or its service centers option and expense, the repair, replacement or refund of the purchase price of any products sold which do not comply with this warranty. Hardware replaced under the terms of this limited warranty may be refurbished or new equipment substituted at Barracuda Networks option. Barracuda Networks obligations hereunder are conditioned upon the return of affected articles in accordance with Barracuda Networks then-current Return Material Authorization ("RMA") procedures. All parts will be new or refurbished, at Barracuda Networks discretion, and shall be furnished on an exchange basis. All parts removed for replacement will become the property of the Barracuda Networks. In connection with warranty services hereunder, Barracuda Networks may at its discretion modify the hardware of the product at no cost to you to improve its reliability or performance. The warranty period is not extended if Barracuda Networks repairs or replaces a warranted product or any parts. Barracuda Networks may change the availability of limited warranties, at its discretion, but any changes will not be retroactive. IN NO EVENT SHALL BARRACUDA NETWORKS LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION.

Exclusions and Restrictions

This limited warranty does not apply to Barracuda Networks products that are or have been (a) marked or identified as "sample" or "beta," (b) loaned or provided to you at no cost, (c) sold "as is," (d) repaired, altered or modified except by Barracuda Networks, (e) not installed, operated or maintained in accordance with instructions supplied by Barracuda Networks, or (f) subjected to abnormal physical or electrical stress, misuse, negligence or to an accident.

EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS MAKES NO OTHER WARRANTY, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO BARRACUDA NETWORKS PRODUCTS, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, AVAILABILITY, RELIABILITY, USEFULNESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS PRODUCTS AND THE SOFTWARE IS PROVIDED "AS IS" AND BARRACUDA NETWORKS DOES NOT WARRANT THAT ITS PRODUCTS WILL MEET YOUR REQUIREMENTS OR BE UNINTERRUPTED, TIMELY, AVAILABLE, SECURE OR ERROR-FREE, OR THAT ANY ERRORS IN ITS PRODUCTS OR THE SOFTWARE WILL BE CORRECTED. FURTHERMORE, BARRACUDA NETWORKS DOES NOT WARRANT THAT BARRACUDA NETWORKS PRODUCTS, THE SOFTWARE OR ANY EQUIPMENT, SYSTEM OR NETWORK ON WHICH BARRACUDA NETWORKS PRODUCTS WILL BE USED WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK.

Software License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE BARRACUDA SOFTWARE. BY USING THE BARRACUDA SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE DO NOT USE THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE

YOU MAY RETURN THE SOFTWARE OR HARDWARE CONTAINING THE SOFTWARE FOR A FULL REFUND TO YOUR PLACE OF PURCHASE.

1. The software, documentation, whether on disk, in read only memory, or on any other media or in any other form (collectively "Barracuda Software") is licensed, not sold, to you by Barracuda Networks, Inc. ("Barracuda") for use only under the terms of this License and Barracuda reserves all rights not expressly granted to you. The rights granted are limited to Barracuda's intellectual property rights in the Barracuda Software and do not include any other patent or intellectual property rights. You own the media on which the Barracuda Software is recorded but Barracuda retains ownership of the Barracuda Software itself.
2. Permitted License Uses and Restrictions. This License allows you to use the Software only on the single Barracuda labeled hardware device on which the software was delivered. You may not make copies of the Software and you may not make the Software available over a network where it could be utilized by multiple devices or copied. You may not make a backup copy of the Software. You may not modify or create derivative works of the Software except as provided by the Open Source Licenses included below. The BARRACUDA SOFTWARE IS NOT INTENDED FOR USE IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, LIFE SUPPORT MACHINES, OR OTHER EQUIPEMENT IN WHICH FAILURE COULD LEAD TO DEATH, PERSONAL INJURY, OR ENVIRONMENTAL DAMAGE.
3. You may not transfer, rent, lease, lend, or sublicense the Barracuda Software.
4. This License is effective until terminated. This License is automatically terminated without notice if you fail to comply with any term of the License. Upon termination you must destroy or return all copies of the Barracuda Software.
5. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE USE OF THE BARRACUDA SOFTWARE IS AT YOUR OWN RISK AND THAT THE ENTIRE RISK AS TO SATISFACTION, QUALITY, PERFORMANCE, AND ACCURACY IS WITH YOU. THE BARRACUDA SOFTWARE IS PROVIDED "AS IS" WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND BARRACUDA HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE BARRACUDA SOFTWARE, EITHER EXPRESSED OR IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR ANY APPLICATION, OF ACCURACY, AND OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. BARRACUDA DOES NOT WARRANT THE CONTINUED OPERATION OF THE SOFTWARE, THAT THE PERFORMANCE WILL MEET YOUR EXPECTATIONS, THAT THE FUNCTIONS WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION WILL BE ERROR FREE OR CONTINUOUS, OR THAT DEFECTS WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION GIVEN BY BARRACUDA OR AUTHORIZED BARRACUDA REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE BARRACUDA SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.
6. License. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOU WILL PROVIDE AN UNLIMITED ZERO COST LICENSE TO BARRACUDA FOR ANY PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS UTILIZED IN THE BARRACUDA SOFTWARE WHICH YOU EITHER OWN OR CONTROL.
7. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL BARRACUDA BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR ABILITY TO USE OR INABILITY TO USE THE BARRACUDA SOFTWARE HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF BARRACUDA HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. In no event shall Barracuda's total liability to you for all damages exceed the amount of one hundred dollars.
8. Export Control. You may not use or otherwise export or re-export Barracuda Software except as authorized by the United States law and the laws of the jurisdiction where the Barracuda Software was obtained.

Energize Update Software License

PLEASE READ THIS ENERGIZE UPDATE SOFTWARE LICENSE CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING BARRACUDA NETWORKS OR BARRACUDA NETWORKS-SUPPLIED ENERGIZE UPDATE SOFTWARE.

BY DOWNLOADING OR INSTALLING THE ENERGIZE UPDATE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM BARRACUDA NETWORKS OR AN AUTHORIZED BARRACUDA NETWORKS RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL PURCHASER.

The following terms govern your use of the Energize Update Software except to the extent a particular program (a) is the subject of a separate written agreement with Barracuda Networks or (b) includes a separate "click-on" license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the written agreement, (2) the click-on agreement, and (3) this Energize Update Software License.

License. Subject to the terms and conditions of and except as otherwise provided in this Agreement, Barracuda Networks, Inc., or a Barracuda Networks, Inc. subsidiary (collectively "Barracuda Networks"), grants to the end-user ("Customer") a nonexclusive and nontransferable license to use the Barracuda Networks Energize Update program modules and data files for which Customer has paid the required license fees (the "Energize Update Software"). In addition, the foregoing license shall also be subject to the following limitations, as applicable:

Unless otherwise expressly provided in the documentation, Customer shall use the Energize Update Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Barracuda Networks equipment) for communication with Barracuda Networks equipment owned or leased by Customer; Customer's use of the Energize Update Software shall be limited to use on a single hardware chassis, on a single central processing unit, as applicable, or use on such greater number of chassis or central processing units as Customer may have paid Barracuda Networks the required license fee; and Customer's use of the Energize Update Software shall also be limited, as applicable and set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation, or web site, to a maximum number of (a) seats (i.e. users with access to the installed Energize Update Software), (b) concurrent users, sessions, ports, and/or issued and outstanding IP addresses, and/or (c) central processing unit cycles or instructions per second. Customer's use of the Energize Update Software shall also be limited by any other restrictions set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation or web site for the Energize Update Software.

General Limitations. Except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

1. transfer, assign or sublicense its license rights to any other person, or use the Energize Update Software on unauthorized or secondhand Barracuda Networks equipment, and any such attempted transfer, assignment or sublicense shall be void;
2. make error corrections to or otherwise modify or adapt the Energize Update Software or create derivative works based upon the Energize Update Software, or to permit third parties to do the same; or
3. decompile, decrypt, reverse engineer, disassemble or otherwise reduce the Energize Update Software to human-readable form to gain access to trade secrets or confidential information in the Energize Update Software.

Upgrades and Additional Copies. For purposes of this Agreement, "Energize Update Software" shall include (and the terms and conditions of this Agreement shall apply to) any Energize Update upgrades, updates, bug fixes or modified versions (collectively, "Upgrades") or backup copies of the Energize Update Software licensed or provided to Customer by Barracuda Networks or an authorized distributor/reseller for which Customer has paid the applicable license fees. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY SUCH ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL ENERGIZE UPDATE SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE; (2) USE OF UPGRADES IS LIMITED TO BARRACUDA NETWORKS EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE ENERGIZE UPDATE SOFTWARE WHICH IS BEING UPGRADED; AND (3) USE OF ADDITIONAL COPIES IS LIMITED TO BACKUP PURPOSES ONLY.

Energize Update Changes. Barracuda Networks reserves the right at any time not to release or to discontinue release of any Energize Update Software and to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, general availability or other characteristics of any future releases of the Energize Update Software.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Energize Update Software in the same form and manner that such copyright and other proprietary notices are included on the Energize Update Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Energize Update Software without the prior written permission of Barracuda Networks. Customer may make such backup copies of the Energize Update Software as may be necessary for Customer's lawful use, provided Customer affixes to such copies all copyright, confidentiality, and proprietary notices that appear on the original.

Protection of Information. Customer agrees that aspects of the Energize Update Software and associated documentation, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Barracuda Networks. Customer shall not disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Barracuda Networks. Customer shall implement reasonable security measures to protect and maintain the confidentiality of such trade secrets and copyrighted material. Title to Energize Update Software and documentation shall remain solely with Barracuda Networks.

Indemnity. Customer agrees to indemnify, hold harmless and defend Barracuda Networks and its affiliates, subsidiaries, officers, directors, employees and agents at Customer's expense, against any and all third-party claims, actions, proceedings, and suits and all related liabilities, damages, settlements, penalties, fines, costs and expenses (including, without limitation, reasonable attorneys fees and other dispute resolution expenses) incurred by Barracuda Networks arising out of or relating to Customers (a) violation or breach of any term of this Agreement or any policy or guidelines referenced herein, or (b) use or misuse of the Barracuda Networks Energize Update Software.

Term and Termination. This License is effective upon date of delivery to Customer of the initial Energize Update Software (but in case of resale by a Barracuda Networks distributor or reseller, commencing not more than sixty (60) days after original Energize Update Software purchase from Barracuda Networks) and continues for the period for which Customer has paid the required license fees. Customer may terminate this License at any time by notifying Barracuda Networks and ceasing all use of the Energize Update Software. By terminating this License, Customer forfeits

any refund of license fees paid and is responsible for paying any and all outstanding invoices. Customer's rights under this License will terminate immediately without notice from Barracuda Networks if Customer fails to comply with any provision of this License. Upon termination, Customer must cease use of all copies of Energize Update Software in its possession or control.

Export. Software, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Energize Update Software.

Restricted Rights. Barracuda Networks' commercial software and commercial computer software documentation is provided to United States Government agencies in accordance with the terms of this Agreement, and per subparagraph "(c)" of the "Commercial Computer Software - Restricted Rights" clause at FAR 52.227-19 (June 1987). For DOD agencies, the restrictions set forth in the "Technical Data-Commercial Items" clause at DFARS 252.227-7015 (Nov 1995) shall also apply.

No Warranty. The Energize Update Software is provided AS IS. Customer's sole and exclusive remedy and the entire liability of Barracuda Networks under this Energize Update Software License Agreement will be, at Barracuda Networks option, repair, replacement, or refund of the Energize Update Software.

Renewal. At the end of the Energize Update Service Period, Customer may have the option to renew the Energize Update Service at the current list price, provided such Energize Update Service is available. All initial subscriptions commence at the time of sale of the unit and all renewals commence at the expiration of the previous valid subscription.

In no event does Barracuda Networks warrant that the Energize Update Software is error free or that Customer will be able to operate the Energize Update Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the Energize Update Software or any equipment, system or network on which the Energize Update Software is used will be free of vulnerability to intrusion or attack.

DISCLAIMER OF WARRANTY. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

General Terms Applicable to the Energize Update Software License Disclaimer of Liabilities. IN NO EVENT WILL BARRACUDA NETWORKS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE ENERGIZE UPDATE SOFTWARE EVEN IF BARRACUDA NETWORKS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Barracuda Networks' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

This Energize Update Software License shall be governed by and construed in accordance with the laws of the State of California, without reference to principles of conflict of laws, provided that for Customers located in a member state of the European Union, Norway or Switzerland, English law shall apply. The United Nations Convention on the International Sale of Goods shall not apply. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Energize Update Software License shall remain in full force and effect. Except as expressly provided herein, the Energize Update Software License constitutes the entire agreement between the parties with respect to the license of the Energize Update Software and supersedes any conflicting or additional terms contained in the purchase order.

Open Source Licensing

Barracuda products may include programs that are covered by the GNU General Public License (GPL) or other "open source" license agreements. The GNU license is re-printed below for your reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks.

GNU GENERAL PUBLIC LICENSE, (GPL) Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public

License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions

will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Barracuda Products may contain programs that are copyright (c)1995-2005 International Business Machines Corporation and others. All rights reserved. These programs are covered by the following License:

"Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation."

Barracuda Products may include programs that are covered by the BSD License: "Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE."

Barracuda Products may include the libspf library which is Copyright (c) 2004 James Couzens & Sean Comeau All rights reserved. It is covered by the following agreement: Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS MAKING USE OF THIS LICENSE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Products may contain programs that are Copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact Office of Technology Transfer Carnegie Mellon University 5000 Forbes Avenue Pittsburgh, PA 15213-3890 (412) 268-4387, fax: (412) 268-7395 tech-transfer@andrew.cmu.edu .Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>)." CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Barracuda products may include programs that are covered by the Apache License or other Open Source license agreements. The Apache license is re-printed below for you reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks.

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License.

You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the

Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Source Code Availability

Per the GPL and other "open source" license agreements the complete machine readable source code for programs covered by the GPL or other "open source" license agreements is available from Barracuda Networks at no charge. If you would like a copy of the source code or the changes to a particular program we will gladly provide them, on a CD, for a fee of \$100.00. This fee is to pay for the time for a Barracuda Networks engineer to assemble the changes and source code, create the media, package the media, and mail the media. Please send a check payable in USA funds and include the program name. We mail the packaged source code for any program covered under the GPL or other "open source" license.